UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

PROPUESTA DE UNA METODOLOGÍA FORENSE PARA LA REALIZACIÓN DE UNA INVESTIGACIÓN FORENSE APLICADA A UN CASO PRÁCTICO.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

ESTHER SELENE MORALES GONZÁLEZ.

DIRECTOR DE TESIS:
M.C LEOBARDO HERNÁNDEZ AUDELO

2012

Agradecimientos.

Al Maestro en Ciencias Leobardo Hernández Audelo
Por ser guía en la realización de este trabajo.

A mis sinodales.
Ing. José Manuel Quintero Cervantes, M. en C. Marcelo Pérez Medel, M. en C. Jesús Hernández Audelo, M. en C. Felipe de Jesús Gutiérrez López por sus valiosas recomendaciones que me ayudaron a lograr el objetivo.

A mi familia.
A mi mamá por tu apoyo incondicional, tus sabios consejos, tu amor ilimitado y tus atinadas correcciones, a mi papá por tu compromiso y por brindarme las condiciones y el amor necesario para ver cumplidos mis sueños.

A Iyari por tu cooperación y buen ánimo, a Héctor por tu ayuda y tu alegría, a Francko por tu apoyo, comprensión y desvelos.

A mis compañeros y amigos.
Por hacer del recorrido una inmejorable experiencia, siempre lleno de alegrías y apoyo.

A todos ustedes muchas gracias

Índice.

Índice de tablas.

Índice de figuras.

Introducción.

En la última década se ha visto un crecimiento acelerado en el área de tecnologías de la información, el número de aplicaciones y lugares donde se utilizan ha aumentado considerablemente trayendo como consecuencia que mucha información ahora se encuentre de forma digital, almacena en algún dispositivo electrónico, lo cual ha cambiado por completo la concepción del trabajo, el entretenimiento, la educación, la política, el comercio… inherente a este cambio se tiene la renovación de las prácticas indebidas.

Las redes y las nuevas tecnologías han brindado un medio al atacante en donde este cuenta con anonimato y la posibilidad de atacar a un gran número de personas desde un solo punto, lo cual ha traído como consecuencia que los delitos al interior de la red superen en un 100% a los que suceden en el mundo físico.

Es por esto que cuando se realiza un crimen es común encontrar que la información referente a este se encuentra almacenada de forma digital en dispositivos electrónicos. Enfrentarse a estos nuevos escenarios significa poder identificar, recuperar, preservar y analizar la evidencia que se encuentre almacenada en estos dispositivos electrónicos, para lo cual se requiere emplear nuevas técnicas, conocimientos y mecanismos que garanticen buenos resultados.

Es en este punto donde nace el cómputo forense, como una ciencia garante de la justicia ante estas nuevas escenas del crimen. Identificando, recuperando, preservando y analizando la evidencia encontrada en los dispositivos.

La presente investigación tiene como campo de interés el cómputo forense, ciencia que está adquiriendo una gran importancia dentro del área de la seguridad informática debido al aumento del valor de la información.

Esta investigación tiene como fin la creación de una metodología para la realización de una investigación de cómputo forense que sea capaz de responder a las necesidades y nuevos retos que esta ciencia presenta.

Se lleva a cabo en el Laboratorio de Seguridad Informática de la Facultad de Estudios Superiores Aragón –FES Aragón- bajo la guía del M. en C. Leobardo Hernández Audelo.

Para lograr la creación de una metodología que respondiera a los retos y necesidades que se presentan durante una investigación de cómputo forense fue necesario hacer el análisis de las principales metodologías con las que se cuenta actualmente.

La metodología resultante del análisis fue implementada en un caso práctico y real, presentado en una institución bancaria. El caso fue trabajado en el Laboratorio de Seguridad Informática de la FES Aragón y llevado ante la correspondiente instancia legal.

La presente investigación tiene la siguiente estructura: consta de seis capítulos; en el capítulo primero “Referentes teóricos” se encontraran los conceptos teóricos de seguridad informática, necesarios para entender las actividades realizadas durante una investigación de cómputo forense.

En el capítulo segundo “Cómputo Forense” está enfocado a los objetivos, principios y etapas que tiene el cómputo forense. Este capítulo servirá para poder plantear el análisis de las metodologías enfocadas a la realización de una investigación de cómputo forense.

En el capítulo tercero “Análisis comparativo de metodología forenses” se hace el análisis de las principales metodologías de cómputo forense que sirvieron como referentes para la creación de la metodología propuesta en este trabajo.

En el capítulo cuarto “Propuesta de metodología para realizar una investigación forense” se presenta la metodología propuesta resultado del análisis

hecho en el capítulo anterior. En este capítulo se encuentra descrito a detalle cada uno de las fases que componen esta la metodología propuesta.

En el capítulo quinto “Metodología propuesta aplicada a un caso práctico” se hace la descripción de las actividades realizadas durante la investigación realizada a un sistema bancario, estas se encuentran organizadas según las fases propuestas en el capítulo cuarto.

Y por último en el capítulo sexto “Resultados y conclusiones” se encuentran tanto los resultados obtenidos del aporte de la metodología forense como los resultados obtenidos al emplear la metodología propuesta para la resolución del caso práctico de investigación de cómputo forense.

Las conclusiones son presentadas en tres líneas rectoras: la primera es la necesidad de concientización del uso de medios digitales, la segunda relacionada con los crímenes digitales; el cómputo forense y el procedimiento legal y por último las conclusiones obtenidas del análisis del sistema bancario.

En la parte de Anexos se encuentra el reporte entregado como resultado de la investigación, mismo reporte que fue entregado ante la parte legal para su fallo.

Capítulo Primero
Referentes Teóricos.

La presente investigación tiene como campo de interés el cómputo forense, el cual se aplica en el momento en que se registra un incidente donde se ven involucrados dispositivos que almacenan información de forma digital.

En las últimas décadas las empresas han tenido pérdidas millonarias debido a incidentes de seguridad; los cuales afectan: sus sistemas, servicios, instalaciones y provocan desde una denegación de servicio, pérdida de información, confidencialidad hasta la pérdida total de la empresa. Estos riesgos pueden mitigarse con el apoyo de una cultura de la seguridad. Existen diferentes tipos de conceptos referentes: a la seguridad, ataques, vulnerabilidades y servicios, que se analizan en este capítulo

1. Seguridad informática

Cada vez es más común encontrar que la información deja de ser almacenada en grandes archiveros para guardarla en un sistema de cómputo de manera digital y con acceso desde diferentes puntos y por diferentes personas; como consecuencia los escenarios de comunicación han cambiado requiriendo implementar seguridad para proteger la información.

1.1 Concepto de Seguridad Informática.

Más personas tienen acceso a la misma información sin importar su ubicación geográfica a través de un sistema de red en donde por medio de la conexión de computadoras se logra la comunicación y transferencia de información. También tenemos sistemas móviles que cuentan con la opción de comunicación en red como lo son los teléfonos celulares, las tabletas electrónicas como: la i-pad de Mac, la playbook de BlackBerry o la kindlefire de Amazon o bien las consolas de videojuegos y ahora hasta SmartTv.; viendo una clara tendencia a que estos sistemas no solo se vuelvan más sofisticados sino que amplíen sus capacidades de comunicación, interconexión y acceso a una mayor cantidad de usuarios.

Esto hace que mantener los servicios de seguridad sea cada vez más complicado, porque el campo que hay que asegurar es más grande y el número de riesgos aumenta.

En México según resultados del estudio realizado por la empresa Norton-Symatec, 83% de los adultos en línea han sido víctimas de los delitos de bandas organizadas, al menos una vez en su vida, y el 79% en el último año. También señala que los cibercrímenes más comunes son: con el 71% el software malicioso y los virus informáticos, con el 17% el phishing o ingeniería social y con el 12% las estafas en línea; a pesar de que solo el 37% de los usuarios adultos de internet no cuentan con software de seguridad actualizado.

Los delitos al interior de la red superan en 100% a los que suceden en el mundo físico y esto se debe a que en este medio el atacante ha encontrado la forma de atacar a un mayor número de personas desde un solo punto bajo el anonimato

Ante la alta probabilidad de ataques cibernéticos hay que precisar que un antivirus no es lo mismo que seguridad informática.

Como definición se dice que la seguridad informática es: un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza. Un proceso en el cual participan además personas. [Aguirre 2006]

El compromiso de la seguridad informática entonces es evitar que todos estos ataques surtan efecto y comprometan al sistema dañando los activos de la entidad[1] y así preservar lo más que se pueda los servicios de autenticidad, confidencialidad, integridad y disponibilidad, protegiendo tanto la infraestructura como la información contenida en ella.

Como métodos para poder implementar seguridad encontramos estándares, protocolos, buenas prácticas, herramientas, entre otras. Es importante mencionar que con todo esto lo que se logra es minimizar el riesgo y no la obtención de un sistema completamente seguro.

[1] Llamaremos entidad a una persona, computadora, un sector de la computadora o bien una compañía o empresa.

1.2. Servicios y mecanismos de seguridad

Ahora que sabemos que es imprescindible implementar seguridad en los diferentes sistemas. Necesitamos saber cuál es la forma correcta de hacerlo.

En el estándar internacional ISO 7498-2 se definen cinco servicios de seguridad y los diferentes mecanismos para implementarlos. Para saber qué clase de servicio es el adecuado para un sistema, hay que tener claro que actividad o información se desea proteger y de qué; los mecanismos serán el cómo se implementara el servicio.

Los servicios son: Autenticación, control de acceso, confidencialidad, integridad y no repudio.

1.2.1. Autenticación

Si se desea tener la certeza de que las partes que interactúan en la comunicación son quienes dicen ser entonces requerimos del servicio de autenticación. Existen dos formas de autenticar a estas partes: la primera es por su identidad y la segunda por el origen de sus datos.

La autenticación de identidad se divide en tres tipos, considerando los elementos que se utilizan para poder implementarla: autenticación por medio de algo que se sabe, autenticación por algo que se tiene y autenticación por algo que se es.

Consideremos el primer tipo. Autenticación por algo que se sabe. Una contraseña es algo que se memoriza, *algo que se sabe,* con respecto a la autenticación por algo que *se tiene,* puede ser una tarjeta electrónica, forzosamente tendrá que ser un objeto físico, por último tenemos el tipo de

autenticación por algo que *se es,* el cual tiene que ver con las características inherentes de las personas: una huella digital, el iris del ojo etc.

Todos los anteriores son autenticaciones por identidad. El otro tipo de autenticación que tenemos es la autenticación de origen de datos, se requiere si lo que deseamos autenticar es el lugar desde donde salieron los datos. Es decir asegurarnos de que el lugar de salida de datos sea el que dice ser.

Los mecanismos utilizados para garantizar el servicio de autenticación son: el cifrado y la firma digital.

1.2.2. Control de acceso.

Si lo que se quiere es proteger a los activos del sistema de la entrada y uso no autorizado. Entonces el servicio indicado es el control de acceso.

Con este servicio podemos administrar a los diferentes usuarios del sistema las actividades que puede y no puede hacer dentro del sistema. Para poder implementar este servicio se utilizan mecanismos específicos de control de acceso.

1.2.3. Integridad.

Cuando la prioridad es mantener la información sin ningún tipo de alteración ya sea por creación, borrado o modificación de forma no autorizadas; requerimos del servicio de integridad. El cual se puede garantizar a través de los mecanismos de cifrado, firma digital y mecanismos específicos de Integridad.

Dentro de la actividad del cómputo forense, que es la parte central de este trabajo, el servicio de integridad es uno de los servicios de los que no se puede prescindir, porque el resultado de la investigación depende de que la evidencia referente permanezca integra durante todo el proceso.

1.2.4. Confidencialidad.

Si lo más importante para nosotros es que la información sólo sea accedida por personas autorizadas, entonces necesitaremos implementar el servicio de confidencialidad.

Tanto el servicio de control de acceso como el de confidencialidad están relacionados con el acceso a personas autorizadas y ambos pueden proporcionarse mediante mecanismos de control de acceso. Sin embargo el servicio de control de acceso autoriza la entrada al sistema, por ejemplo, pero no necesariamente permite acceder a toda la información que se tiene almacenada, siguiendo con nuestro ejemplo, el servicio de confidencialidad además permite el acceso a información clasificada.

La confidencialidad se garantiza mediante la aplicación de los mecanismos de cifrado y control de acceso.

1.2.5. No repudio.

Cuando lo que queremos garantizar es que, alguna de las partes involucradas en la comunicación, no pueda negar que envío o recibido algún mensaje. Entonces los que necesitamos es el servicio de no repudio. Existen dos servicios de no repudio: los de prueba de origen y los de prueba de entrega.

Este servicio se puede garantizar mediante los mecanismos de firma digital y mecanismos específicos de Integridad.

La tabla 1.1 presenta los cinco servicios mencionados anteriormente y los mecanismos con los que se pueden implementar.

Tabla 1.1 Servicios y mecanismos de seguridad.

Servicios de Seguridad	Capa de aplicación (OSI)	Mecanismos							
		Cifrado	Firma digital	Control de acceso	Integridad	Autenticación	Trafficpadding	Control de ruteo	Notarización
Autenticación por identidad	3,4,7	Si	Si			Si			
Autenticación por origen de datos	3,4,7	Si	Si						
Control de acceso	3,4,7			Si					
Confidencialidad con conexión y sin conexión	2,3,4,7	Si						Si	
Confidencialidad selectiva de campo	7	Si							
Confidencialidad de flujo de tráfico	1,3,7	Si					Si	Si	
Integridad con conexión con o sin recuperación	4,7	Si			Si				
Integridad con conexión selectiva de campo	7	Si			Si				
Integridad sin conexión	3,4,7	Si	Si		Si				
Integridad sin conexión y selección de campo	7	Si	Si		Si				
No repudio de origen y de entrega	7		Si		Si				Si

Cuando se piensa en la creación de un sistema es importante que también se piense en los servicios de seguridad que requiere y en que parte los necesita o para que actividades, todo esto derivado del análisis de riesgos, él cual nos dirá cuales son los activos que se deben de proteger, las vulnerabilidades del sistema y las amenazas que este puede presentar; ya que no todos los sistemas necesitan los mismos servicios ni necesitan implementarse todos.

1.3. Vulnerabilidad, Amenazas y Riesgo.

Para los usuarios de un sistema (cómputo, móviles…) es muy importante saber cómo identificar sus vulnerabilidades, conocer el tipo de amenazas que existen y el comportamiento del atacante.

Las últimas estadísticas publicadas por Symantec, las cuales corresponden al estudio realizado a 24 países, durante el año 2011, muestran que las pérdidas que se han tenido debido al cibercrimen alcanzaron los 388.000 millones de dólares los cuales se perdieron en solo 12 meses. Teniendo así al año 431 millones de adultos en línea que sufrieron ataques de cibercrimen es decir más de un millón de adultos al día; 14 víctimas por segundo. Esto hace que para todos los adultos en línea aumente el riesgo de ser atacados en un 44% (*Véase fig. 1.1)*.

Figura 1.1 Estadística publicada por Symantec. 2011.

Por primera vez este informe revela que el 10% de todos los adultos en línea encuestados han sufrido ataques de cibercrimen en sus dispositivos móviles.

La característica de movilidad permite al usuario una conexión continua que le facilita las tareas diarias de su trabajo y opciones de entretenimiento, pero lo expone a ser atacado un mayor número de horas, por lo tanto la probabilidad de ser atacado aumenta y la vulnerabilidad es mayor.

Todos estos datos definitivamente nos tendrían que hacer pensar en: ¿Qué es lo que estamos haciendo mal como usuarios?, ¿realmente estamos enterados de los riegos que presenta nuestro sistema?, ¿nos preocupamos por saber cuáles sus vulnerabilidades y las amenazas que existen para cada una de ellas? y ¿Qué hacer para protegerlo?

Lo lamentable es que muchas veces este tipo de preguntas no se hacen cuando se pone en marcha un sistema, sino hasta después de que un ataque es exitoso habiendo explotado alguna de sus vulnerabilidades y provocando pérdidas. Que es justamente el momento en el que se requiere la ayuda del cómputo forense para poder saber qué es exactamente lo que sucedió.

Sin embargo se pueden prever ataques y todo lo que esto conlleva teniendo información sobre vulnerabilidad, ataques, amenazas y riesgos. Por lo cual definiremos cada uno de estos conceptos.

Vulnerabilidad es cualquier tipo de debilidad o fallo interno o externo que posea el sistema y que pueda ser explotada con el fin de causar pérdida o daño a éste.

Muchas de las vulnerabilidades que son explotadas para dañar un sistema son vulnerabilidades propias de las aplicaciones o sistemas operativos (S.O). Por lo cual es recomendable antes de hacer la instalación de las aplicaciones o S.O conocer sus vulnerabilidades a través de un ambiente controlado, en el cual se le puedan realizar pruebas y verificar cual es la configuración adecuada. Si no es posible mitigar los riegos de una amenaza es preferible no hacer la instalación. Lo

que se debe evitar definitivamente es instalar una aplicación con la configuración que trae de fábrica.

Existen sitios que se dedican a publicar vulnerabilidades de diferentes aplicaciones y S.O, si se requiere proteger un sistema es importante tener esta información, así como mantener los sistemas actualizados aprovechando las mejoras en seguridad por parte del proveedor.

Otras vulnerabilidades que presentan los sistemas son:

- Falta de claridad en las políticas.
- Falta de análisis de riesgos.
- Ausencia de la autenticación de usuarios.
- Robos y pérdidas.
- Falta de responsabilidad de los usuarios.
- Falta de respaldos de información.
- Falta de políticas de acceso remoto.
- Bitácoras limitadas.

Amenaza es cualquier circunstancia que pueda causar pérdida o daño al sistema. Existen dos tipos de amenazas: naturales y humanas.

En el caso de las naturales: un incendio, una inundación, un tornado, un huracán, etc.

Dentro de las humanas tenemos las accidentales y las intencionales. Como accidentales, todas aquellas acciones que tengan que ver con la negligencia y la ignorancia humana: el envío equivocado de mensajes, entrega de llaves a personas equivocadas, apagado de servidores por falta de conocimiento... Las

intencionales se refiere a acciones premeditadas: el robo de dispositivos, acceso no autorizado, el robo de información, el apagado intencional de servidores, instalación de software malicioso, etc.

Sin embargo cuando hablamos de un sistema de cómputo, los activos más importantes que tenemos que proteger son los datos, los programas y los equipos.

Los sistemas de cómputo tienen cuatro principales tipos de amenazas que son: la interrupción, la intercepción, la alteración y la fabricación. Estas amenazas van dirigidas a modificar o inhibir el flujo deseable de la información.

A continuación se esquematiza cada una de ellas dentro del flujo normal o deseable de la información (*Véase fig. 1.2)*, en el cual tendremos dos actores principales. Estos son:

- El origen
- El destino.

Figura 1.2 Flujo normal.

Interrupción. Esta amenaza va dirigida a bloquear la disponibilidad de la información o servicio dejando así la pérdida o inutilidad del activo. Esto lo logra con la destrucción o daño en algún elemento del sistema que contenga o proporcione la información, puede ser el daño de un disco duro, el corte de las líneas de comunicación (cables de red), la alteración al sistema de gestión de archivos etc. (*Véase fig. 1.3).*

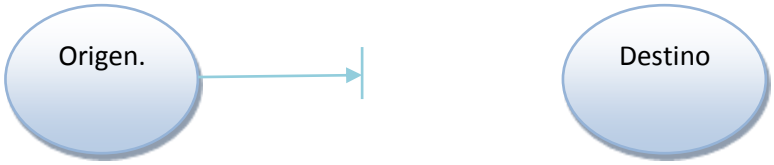


Figura 1.3 Amenaza de Interrupción.

Intercepción. Esta es una amenaza a la confidencialidad en la cual se busca tener acceso a la información o servicio de una manera ilícita. La parte que genera la intercepción no necesariamente tiene que ser una persona, puede ser un programa. Algunos ejemplos de esta amenaza son: el acceso no autorizado a un sistema, la copia ilícita de archivos o programas, la intercepción de comunicaciones con el fin de capturar tráfico, un espía escuchando una conversación, etc. (*Véase fig. 1.4).*

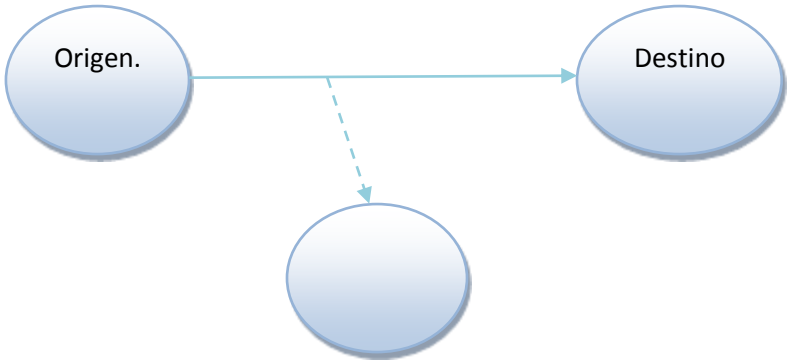


Figura 1.4 Amenaza de Intercepción.

Alteración. Esta es una amenaza a la Integridad. Se da cuando hay una modificación en algún archivo o programa de manera no autorizada, esto con el fin de alterar el comportamiento del sistema. Algunos ejemplos son cuando se alteran los paquetes transmitidos por la red, cuando se altera los archivos de contraseñas para poder tener acceso con el perfil de otro usuario, el cambio de datos en base de datos, alteración de programas para que realicen alguna actividad específica, etc. (*Véase fig. 1.5).*

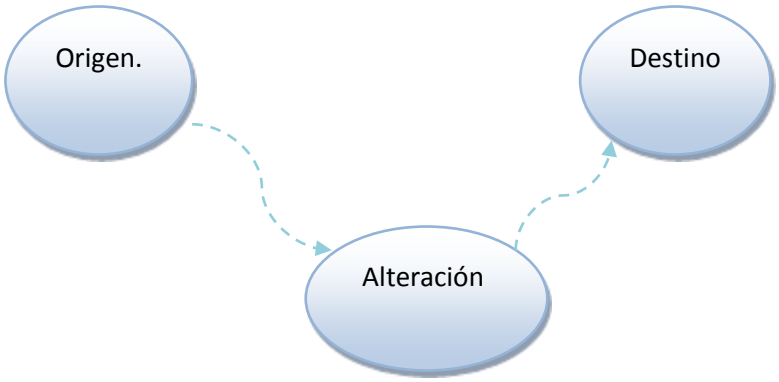


Figura 1.5 Amenaza de Alteración.

Fabricación. Esta es otra amenaza a la integridad en donde se crea de manera ilícita archivos en el sistema o paquetes en el tráfico de red. Ejemplos: inserción de transacciones en un sistema, agregar registros a una base de datos, etc. (*Véase fig. 1.6).*

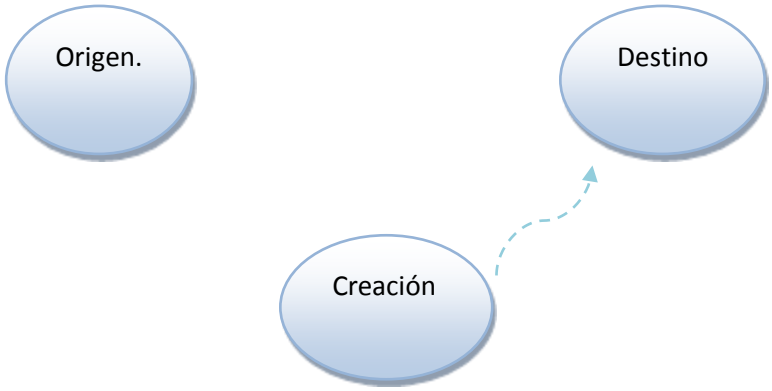


Figura 1.6 Amenaza de Fabricación.

Riesgo es la probabilidad de que una vulnerabilidad de la infraestructura sea explotada por una amenaza (Peltier 2005). Existirán amenazas y vulnerabilidades que no representen un riesgo, es decir que la probabilidad de que sucedan sea

muy baja o bien que la parte del sistema que afecten no forme parte de sus activos. Disminuir un riesgo es más productivo que eliminar vulnerabilidades.

Se pueden disminuir los riegos de un ataque haciendo un análisis del sistema (análisis de riesgo) el cual arroje sus vulnerabilidades, las amenazas que presenta, la probabilidad de que cada una de ellas suceda y el costo de que la vulnerabilidad se vea explotada.

Realizar un análisis de riegos nos da la pauta para poder implementar mecanismos y políticas de seguridad que garanticen protección a los activos de manera eficaz, optimizando tiempo y recursos.

Todas estas acciones disminuyen riegos pero los usuarios representan el factor más complicado, siendo las amenazas humanas actualmente inevitables.

Es importante en esta era de la información tomar conciencia de la importancia de una contraseña, de la responsabilidad que representa el uso de sistemas que guardan información sensible, de respetar las políticas en beneficio de una comunidad que puede progresar a través del uso adecuado de medios computacionales.

Actualmente es prioritario tener información sobre el sistema que elijas utilizar, considerar los riegos que representa su uso y prever de manera responsable los alcances de un uso inadecuado.

1.3.1. Elementos de un Sistema de cómputo y sus principales amenazas.

Es importante ubicar las principales amenazas en los diferentes elementos que conforman el sistema.

De manera general podemos especificar cuatro elementos dentro de un sistema de cómputo. Estos son:

- Software.
- Hardware.
- Datos.
- Líneas de comunicación.

Las amenazas van dirigidas a estos elementos, dañando a uno o más a la vez.

Empezaremos con el *Software,* en este caso veremos que la mayoría de las amenazas que se presentan van dirigidos a bloquear la disponibilidad, esto se logra dañándolo, alterándolo o eliminándolo, lo cual provoca la denegación del acceso autorizado de los usuarios al sistema (denegación de servicio).

Sin embargo no es el único tipo de amenaza hacia el software, también tenemos amenazas que dañan la confidencialidad y la integridad. Por ejemplo: se viola la confidencialidad al realizar copias no autorizadas del software, y se viola la integridad al alterar un programa para que este se comporte de alguna manera en específico. Esta última es una de las acciones más utilizadas por el malware.

En el caso del *Hardware* este es susceptible a las amenazas dentro del campo de la disponibilidad. Esto se produce cuando existen daños accidentales o deliberados a los equipos como puede ser el robo o daños físicos (golpes).

Los *datos* son susceptibles a amenazas que dañan la disponibilidad, la confidencialidad y la integridad principalmente. Siendo la confidencialidad de los datos uno de los servicios más requeridos. Este servicio se ve violado no sólo con el acceso a los archivos sino también deduciendo su contenido a partir de la creación de bases de datos y de estadísticas que de ellas se generan, así de información global se puede obtener información de particulares.

Aunque la creación de base de datos y estadísticas sea más complicada o requiera más tiempo, en ciertos casos puede ser más viable que pretender el acceso a un documento protegido.

Pero la confidencialidad no es lo único que se busca alterar cuando de datos se trata, también tenemos amenazas a la integridad como lo son: la modificación de archivos o la alteración o creación de datos dentro de las bases de datos de manera ilícita.

La eliminación de algún dato sin duda sería un daño a la disponibilidad ya que los usuarios no podrían tener acceso a él.

Como último elemento de los sistemas de cómputo tenemos las *Líneas de comunicación* este elemento es el encargado de transportar la información por lo tanto las amenazas estarán dirigidas a interrumpir (disponibilidad), adquirir (confidencialidad) o modificar (integridad) la información. Sólo que por ser un elemento diferente las amenazas se presentaran de otra forma. Por ejemplo mientras que en los datos la interrupción se logra borrando datos en el caso de las líneas de comunicación se podría lograr cortando los cables que utiliza como transporte.

A continuación se muestra una tabla que contiene los elementos del sistema de cómputo y sus principales amenazas así como el servicio que perjudican (*Véase tabla 1.2*).

Tabla 1.2 Principales amenazas a los elementos del sistema de cómputo.

Activos	**Amenazas**	**Servicios**
Hardware	Intercepción (robo) Interrupción	Confidencialidad Disponibilidad
Software	Modificación (malware) Interrupción. Intercepción	Integridad Disponibilidad Confidencialidad
Datos	Modificación Fabricación Intercepción Interrupción	Integridad Integridad Confidencialidad Disponibilidad
Líneas de comunicación	Modificación Fabricación Intercepción Interrupción	Integridad Integridad Confidencialidad Disponibilidad

1.4. Ataques al sistema

En este apartado hablaremos de los tipos de ataques que existen, mencionaremos los más comunes y los pasos que sigue un atacante cuando busca vulnerar un sistema.

El índice de ataques que se registran en todo el mundo crece cada año. Durante el 2011 México fue el país con más ataques de virus informáticos y malware con un 71% (según estadísticas de Symantec), y ocupa el tercer lugar en número de víctimas por cibercrimen con un 83% (*Véase fig.1.7*).

Figura 1.7 Estadísticas de ataques publicadas por Symantec 2011.

Probablemente el número de ataques a un sistema no podamos disminuirlo, es más casi inevitablemente subirá, pero lo que si podemos hacer es que éstos no tengan éxito, para lo cual se requiere tener conocimiento de cuáles son los ataques a los que nos enfrentamos, cómo son operados, cuáles son las vulnerabilidades que atacan y por supuesto conocer las vulnerabilidades de nuestro sistema y el tipo de amenazas a las que está expuesto.

Existe una frase escrita en el libro “El arte de la guerra” que va muy bien con esta lucha por obtener seguridad informática en nuestros sistemas y dice así:

"conoce a tu enemigo, conócete a ti mismo; en cien batallas, nunca saldrás derrotado"[2].

Tener estos conocimientos no sólo sirve para prevenir, en caso de que el ataque tenga éxito podremos seguir los pasos del atacante buscando alguna huella que nos lleve a él y lograr que sus actos tengan una penalización. Esto es uno de los objetivos del cómputo forense.

1.4.1. Tipos de ataques

Existe una clasificación de ataques dependiendo de si estos causan o alteran la comunicación o no. De esta forma tenemos dos tipos de ataques: Los ataques pasivos, y los ataques activos. Muchas veces este tipo de ataques se combinan para lograr su objetivo.

1.4.1.1. Ataque pasivo.

Este tipo de ataques es muy sutil, no altera la comunicación, únicamente la escucha o la monitoriza con el fin de analizar los datos y obtener así algún tipo de información.

Cuando el atacante realiza ataques pasivos puede ser que se encuentre con información cifrada, si es así, no intentará descifrarla, solo recabará los datos que se obtengan de manera inmediata e intentará encontrar vulnerabilidades en el sistema cuidando no alterar de ninguna manera la información.

La información que puede obtener es por ejemplo: quien es el que está mandando el mensaje (probablemente no obtenga el nombre de la persona sino

[2] Frase del libro el arte de la guerra de SunTzu Sólo **ficha bibliográfica y página.**

una ip[3]), hacia quien lo envía, en que horarios se registra la mayor actividad, de que tamaño son los envíos que se hacen. Y así ir estableciendo horarios, trazando esquemas de ubicación de los equipos, puertos abiertos, versiones de los sistemas operativos y saber cuáles son el tipo de aplicaciones que usan.

Este tipo de ataques siempre son la antesala para un ataque activo, le da al atacante información de su víctima, le ayuda a planear mejor la estrategia para poder cumplir su objetivo. Como este tipo de ataques no produce ninguna alteración, detectarlos se vuelve muy complicado. La forma de protegerse de estos ataques es la prevención y no la detección.

A continuación se describen tres ejemplos de ataques pasivos.

1.4.1.1.1 Análisis del tráfico.

Estos ataques buscan observar los datos y el tipo de tráfico que se está transmitiendo por las redes de información, para ello suelen utilizar como herramienta los sniffers diseñados para registrar constantemente el tráfico de la red.

Una forma de protegerse de los sniffers es utilizar redes conmutadas y redes locales virtuales que se encuentre fuera del alcance del sniffer, aunque esto no evita del todo que estos ataques puedan darse ya que existen técnicas que permiten al atacante interceptar el tráfico de todas maneras, sin embargo lo hace más complicado.

1.4.1.1.2. Ingeniería Social.

Este ataque se basa en la premisa de que los usuarios son el eslabón más débil de la cadena. En este tipo de ataques lo que se suele hacer es convencer a

[3] IP es el número de identificación que se le da a una máquina cuando se integra a una red.

un usuario legítimo de dar información del sistema, esto es logrado mediante diferentes técnicas. Las más usadas son las llamadas telefónicas o el envío de correos electrónicos donde el atacante finge ser un técnico, el administrador del sistema, un compañero de trabajo, un empleado de algún banco o cualquier otra identidad que le ayude a que el usuario le proporcione la información que el requiere.

Uno de los ingenieros sociales más famosos es Kevin Mitnick [Willey – 2002], el cual decía que la ingeniería social se basa en cuatro principios.

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir NO.
4. A todos nos gusta que nos alaben.

Este tipo de ataques se puede prevenir con cultura, informando a los usuarios de cuáles son las prácticas de seguridad.

1.4.1.1.3. TEMPEST

Este ataque está basado en que cualquier dispositivo electrónico emite continuamente radiaciones a través del aire o de conductores, la corriente que circula por un conductor produce un campo electromagnético que es capaz de inducir esta misma señal a otros conductores que se encuentren cerca. De esta forma si se cuenta con los equipos necesarios se pueden captar esas transmisiones y reproducir de forma remota como por ejemplo: las imágenes que se están viendo en un proyector, en un monitor de una computadora, los documentos que se envían a las impresoras o las pulsaciones en un teclado.

Existen equipos diseñado especialmente para que las emisiones electromagnéticas que se produzcan sean bajas, sin embargo estos equipos son

muy caros. Pero no es la única forma de prevenir este ataque existen lo que se conoce como jaulas de Faraday que pueden proteger no sólo a un equipo sino a una sala o edificio completo creando zonas electromagnéticas aisladas haciendo imposible captar emisiones que se producen en su interior.

Este principio de las jaulas de Faraday se aplica en el cómputo forense en lo que se conoce como “bolsas de Faraday”, sirven para guardar la integridad de la evidencia evitando que los dispositivos electromagnéticos se vean alterados por algún otro campo electromagnético.

Suelen ser muy útiles cuando la evidencia se encuentra dentro de un celular y requerimos mantenerlo prendido pero sin que presente ninguna alteración, como el celular está constantemente mandando y recibiendo señales tenemos que encontrar una manera de aislarlo sin apagarlo, es aquí cuando una bolsa de Faraday resuelve este problema.

1.4.1.2. Ataque Activo

Los ataques activos son aquellos que alteran el sistema. Modifican el flujo y/o crean un falso flujo de datos. Dentro de este tipo de ataques tenemos cuatro categorías.

- Alteración del flujo. Este es cuando se altera sólo una parte del mensaje legítimo, o bien se reenvían o se reordenan para producir el efecto que el atacante desea.

- Privación del servicio. Este bloquea el uso de las comunicaciones ya sea para un usuario en específico o provocando que el bloqueo sea para todo el sistema.

- Reactuación. Es cuando se hace el envío de un mensaje lícito repetidas veces, provocando el efecto que el atacante desea como por ejemplo

mandar el mensaje de depósito de dinero a una cuenta varias veces cuando el depósito sólo se hizo una vez.

- Suplantación. Esta tiene lugar cuando un atacante finge ser una entidad diferente. Normalmente para lograr un ataque de este tipo antes se tuvo que hacer algún otro tipo de ataque activo.

En estos casos la detección es mucho más sencilla porque los cambios en el flujo de información son evidentes. Se puede mitigar el ataque monitoreando las líneas de comunicación y así detectar inmediatamente el ataque, detenerlo y recuperar lo antes posible el servicio, si es que se vio dañado; así como reforzar la seguridad, evitando que el sistema se vea vulnerado de la misma manera.

A continuación se describen tres tipos de ataques activos.

1.4.1.2.1. Inyección SQL.

Este tipo de ataques va dirigido a alterar, dañar u obtener información de un servidor; lo hace a través de comandos SQL, aprovechándose de algún fallo de seguridad por parte de los diseñadores, programadores y/o administradores. Para que este ataque surta efecto, el servidor deberá contar con algún manejador de base de datos.

En un ataque de inyección SQL se le manda al servidor una consulta en donde se mezcla información de entrada del usuario con comandos SQL para construir una consulta maliciosa.

1.4.1.2.2. Hijacking.

Este es un ataque de suplantación el cual consiste en ocupar la identidad de la víctima de forma no autorizada en algún sistema: ya sea financiero, de correo, modem, o cualquier otro. La forma de lograr esto ya dependerá del ingenio del atacante ya que existen muchas maneras de lograr este fin.

El nombre Hijacking viene de la palabra en ingles hijack que significa secuestro.

1.4.1.2.3 Denegación de servicio.

Este tipo de ataque daña la disponibilidad, inhabilita el servicio proporcionado por alguna entidad, este tipo de ataques puede causar pérdidas millonarias por segundo a aquellas entidades que tengan como modelo de negocio la venta en línea, como lo son: amazon o bestbay.

En 1978 se hizo un estudio por la Universidad de Minesota en donde la mayoría de las empresas podían sobrevivir interrupciones del negocio entre 2 y 6 días. Actualmente según Colleen Gordon público en “Disaster Recovery Journal” que una empresa con autorización de venta por tarjetas de crédito puede perder 2.6 millones de dólares por hora.

1.4.2. Metodología de un ataque.

Para poder realizar un ataque a alguna red o sistema de cómputo el atacante necesita una serie de factores como los son: una motivación, los medios técnicos, herramientas, conocimientos y además contar con una oportunidad que facilite el ataque, puede ser un fallo en el sistema. Todos estos factores constituyen lo que se denomina el “*triángulo de la intrusión” (Véase fig. 1.8).*

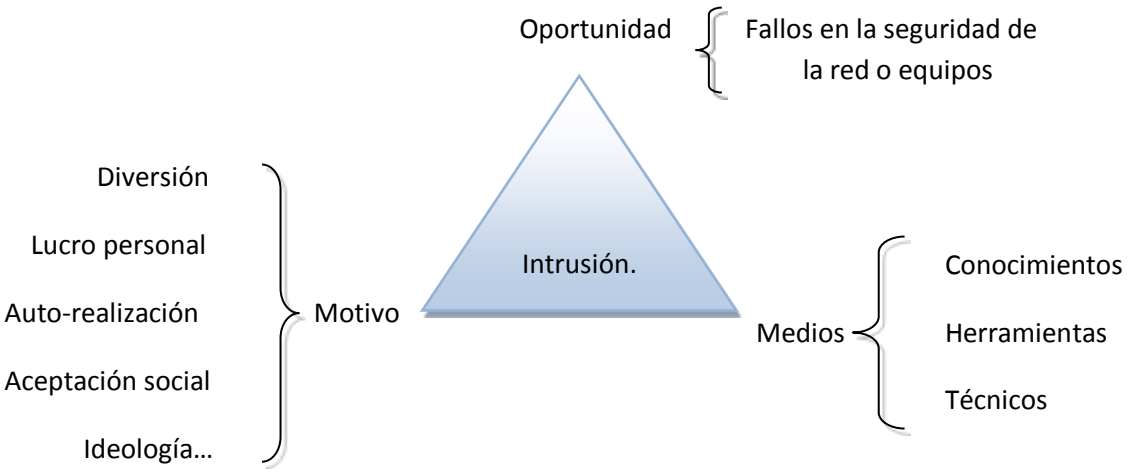


Figura 1.8 Triangulo de la Intrusión.

Los ataques contra redes de computadoras o contra sistemas computacionales que guarden información suelen constar de las siguientes etapas:

1. *Descubrimiento* y exploración del sistema informático es aquí donde se usan ataques pasivos para poder ir descubriendo en qué condiciones se encuentra el sistema que se desea atacar.

2. *Enumeración*. En esta etapa se va recabando toda la información referente al sistema: el tipo de sistema operativo que tiene, los puertos abiertos, tipo de aplicaciones que usa, si cuenta con algún servicio web, que tipo de mecanismos de seguridad usa, etc.

3. *Análisis de vulnerabilidades*. Es en esta etapa donde se hace una matriz de ataque en la cual se ponen todas las características que encontramos en el paso anterior y las vulnerabilidades que este presenta, esto nos dará una clara idea de cuál es el mejor camino para atacar.

4. *Explotación de vulnerabilidades*. En este punto se hace uso de las herramientas que han sido construidas con este fin llamadas *exploits.*

5. *Corrupción y compromiso del sistema*. Una vez que se ha conseguido el acceso al sistema, entonces el atacante produce los cambios, ya sean de modificación, creación, instalación o duplicación. Una vez que ha obtenido acceso al sistema lo más probable es que desee mantenerlo, haciendo la instalación de puertas traseras, las cuales le permitirán volver a entrar al sistema sin dificultades.

   Se pueden generar puertas traseras creando cuentas con privilegios administrativos o bien se escalan privilegios si es que ya tiene alguna cuenta utilizándola como puerta trasera.

6. Por último se hace la *eliminación de pruebas,* en esta etapa el atacante busca borrar todas las pruebas que delaten el ataque al sistema, para lo cual lo más común es que haga modificaciones o eliminaciones de archivos "logs" que son archivos que registran la actividad del equipo.

Conocer los pasos que suele seguir un atacante sirve tanto para prevenirnos, como para analizar el sistema después de que se ha registrado un ataque. De esta forma sabremos cuáles son los lugares dentro del sistema en donde podemos encontrar alguna huella dejada por el atacante.

Un mecanismo muy demandado para poder implementar algún servicio de seguridad es la criptografía ya que garantiza los servicios de: confidencialidad, autenticación de entidad y origen de datos, no repudio e integridad de datos. Por lo que se hace necesario puntualizar generalidades de la criptografía.

2. Criptografía

Es importante tratar el tema de criptografía ya que durante una investigación forense emplearemos ésta para garantizar el servicio de integridad de datos; servicio que tenemos que considerar primordial. La integridad de la evidencia será requisito indispensable para poder ser empleada.

Es probable que la evidencia este cifrada o bien que se desee cifrar para garantizar la confidencialidad, para lo cual la criptografía será una herramienta indispensable. Además a través de la criptografía se pueden garantizar la mayoría de los servicios de seguridad.

2.1. Definición.

Esta palabra proviene del griego “kriptos” que significa oculto y “grafos” escritura, etimológicamente la criptografía es la manera de escribir de un modo secreto. Con respecto a las técnicas que se utilizan en los sistemas informáticos es válido consultar otras definiciones.

Aguirre dice: “La rama de las matemáticas y en la actualidad también de la informática y la telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por lo tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves” [Aguirre - 2006].

Según los autores Menezes, Van Oorschoy y Vanstone “la criptografía es el estudio de técnicas matemáticas relacionadas con los aspectos de la seguridad de la información tales como la confidencialidad, la integridad de datos, la autenticación de entidad y de origen. La criptografía, no comprende sólo a los medios para proveer seguridad de información, sino a un conjunto de técnicas.” [Menezes y Van - 2001].

Se considera que la criptografía moderna nació durante la segunda guerra mundial en donde se construyeron y se utilizaron máquinas de cifrado mecánicas y electromecánicas como ejemplo tenemos la máquina “Enigma”.

La criptografía es un mecanismo utilizado para transformar o cifrar la información de manera que ésta sea irreconocible para aquellas personas no autorizadas.

Esta ciencia se ha seguido desarrollando ahora basada en la teoría de la información, la matemática discreta, la teoría de los grandes números y la ciencia de la computación.

2.2. Usos de la criptografía.

A través de la criptografía se garantizan los siguientes servicios de seguridad:

Confidencialidad o privacidad de la información ha sido la aplicación más antigua de la criptografía. El objetivo en este caso de cifrar un mensaje, es que este pueda viajar en un canal no seguro, almacenado en un dispositivo no seguro y que aún así sólo la persona autorizada tenga acceso al mensaje.

Otro uso que tiene la criptografía es la *autenticación* de entidad y autenticación de origen de datos. En este caso el objetivo es corroborar que la entidad es quien dice ser o bien que los datos provienen de la fuente que dicen provenir.

Usar la criptografía para garantizar el *no repudio* nos previene de qué una entidad niegue un envío previo de información, un mensaje o una acción.

Por último tenemos la aplicación de criptografía para garantizar el servicio de *integridad*, este tipo de aplicación se ha popularizado debido a que existen muchos ataques que modifican programas inofensivos con el fin de engañar a los usuarios, por lo cual es necesario comprobar la integridad de cualquier programa.

Mientras que para proteger un sistema la criptografía es ideal, se convierte en un reto si se trata de una investigación forense porque oculta información que puede servir como evidencia al caso. Para salvar el reto hay que conocer las diferentes formas en que se implementa.

Existen diferentes formas de aplicar este mecanismo. Puede ser con algoritmos de criptografía simétrica o clásica, algoritmos de criptografía asimétrica, o algoritmos de funciones hash.

2.3 Criptografía simétrica.

La criptografía simétrica también es llamada criptografía clásica o convencional en donde sólo tenemos una llave que será la que ocuparemos para cifrar y descifrar el mensaje, esta llave se debe conservar en secreto, por lo que deberá haber un acuerdo de llave entre el emisor y el receptor.

En este tipo de criptografía participan diferentes elementos: emisor, receptor, un mensaje y una llave de cifrado y descifrado. Lo que se realiza es lo siguiente. Tanto el emisor, al que llamaremos “A”, como el receptor, al que llamaremos “B”, conocerán la llave o clave secreta, “A” cifra la información con el algoritmo y la llave o clave acordada para después enviar el mensaje cifrado a “B” por medio de un canal que se considera inseguro. Una vez que B recibe el mensaje cifrado, lo descifra empleando el algoritmo y la clave o llave previamente acordada, de esta manera podrá obtener el mensaje original (*Véase fig.1.9)*.

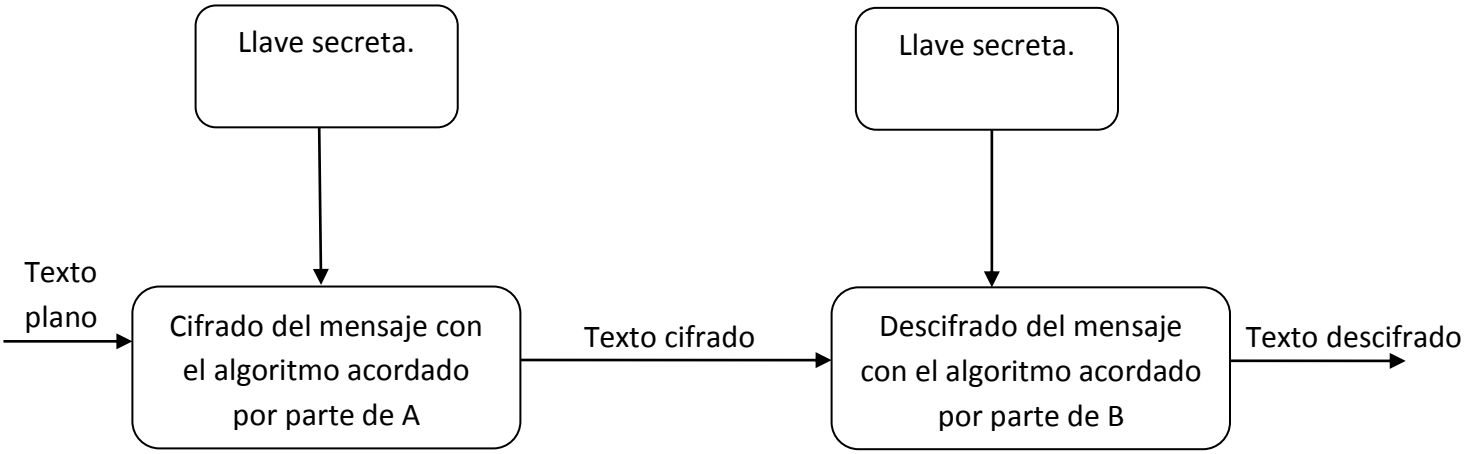


Figura 1.9 Esquema de criptografía simétrica.

Analizando cómo funciona la criptografía simétrica encontramos que presenta tres problemas:

a) El acuerdo de llave. Se tiene que realizar antes de poder usar el protocolo criptográfico de manera segura, lo cual obliga a realizarlo en persona para evitar riesgos al hacerlo a través de un canal inseguro.

b) El manejo de la llave. Al pensar en usar un protocolo criptográfico en una red de “n” usuarios tendremos que usar una clave secreta por cada pareja lo que hace un total de n(n-1)/2 claves para esta red. Lo cual complica tanto la memorización de las claves como la administración de éstas, sin mencionar que por cada par tenemos el problema del acuerdo de llaves.

c) El servicio de autenticación de entidad. No podemos garantizar la autenticación mediante el uso de algún protocolo de criptografía simétrica.

2.4. Criptografía asimétrica.

Con la aparición de la criptografía asimétrica se resuelven los problemas que presenta el uso de la criptografía simétrica.

Diffie y Hellman describieron un protocolo con el cual es posible hacer el acuerdo de llave sin tener presentes a las personas y sin que la llave viaje por el medio.

La criptografía asimétrica es aquella en donde la llave de cifrado es diferente a la clave de descifrado. En este esquema la llave de cifrado es del conocimiento público mientras que la llave de descifrado sólo es conocida por el receptor del mensaje.

En este esquema asimétrico se tendrá como elementos: un emisor, un receptor, dos llaves públicas, dos llaves privadas un mensaje y un algoritmo. En este esquema lo que se hace es que “A” genera su par de llaves, una pública y otra privada, la pública se la manda a “B” la cual a su vez genera su par de llaves y le manda a “A” su llave pública. Posteriormente si “A” desea cifrarle algún mensaje a “B” lo que tendrá que hacer es utilizar su llave pública para cifrar el mensaje y mandárselo a “B”. “B” al recibir el mensaje tendrá que descifrarlo con su llave privada la cual es la única que puede descifrar el mensaje.

Con esto tenemos resueltos los problemas del acuerdo de llave, podemos garantizar los servicios de: no repudio, confidencialidad, autenticación, integridad y nace el concepto de firma digital.

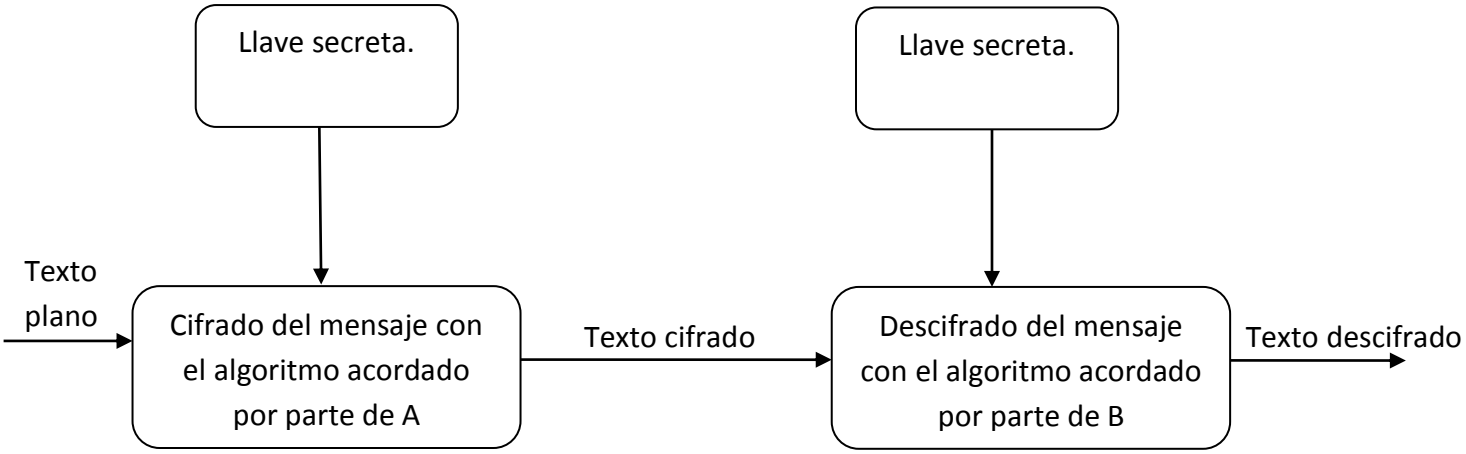


Figura 1.10 Esquema de criptografía asimétrica.

Para poder implementar algún servicio de seguridad por medio de la criptografía muchas veces esta se apoya en el uso de funciones hash

Estas funciones no son utilizadas para cifrar información ni son consideradas como un protocolo criptográfico sin embargo es una parte fundamental de muchos algoritmos criptográficos. Se verá algo sobre funciones hash.

2.5. Funciones hash.

Las funciones hash son también llamadas funciones de una vía, funciones resumen o funciones de digestión. Estas funciones obedecen a un algoritmo matemático y tienen como entrada un conjunto de elementos -generalmente cadenas- y una salida de tamaño fijo -normalmente una cadena- poseen las siguientes características:

Una función hash es *Inyectiva*, cada elemento de entrada debe obtener un elemento de salida diferente Es decir para cada uno de los elementos que conformen el conjunto de “elementos de entrada” le corresponderá un sólo elemento del conjunto de “elementos de salida” tal que dentro del conjunto de “elementos de entrada” no puede haber dos o más elementos que tengan el mismo elemento de salida. Guarda las mismas propiedades que una función inyectiva matemática.

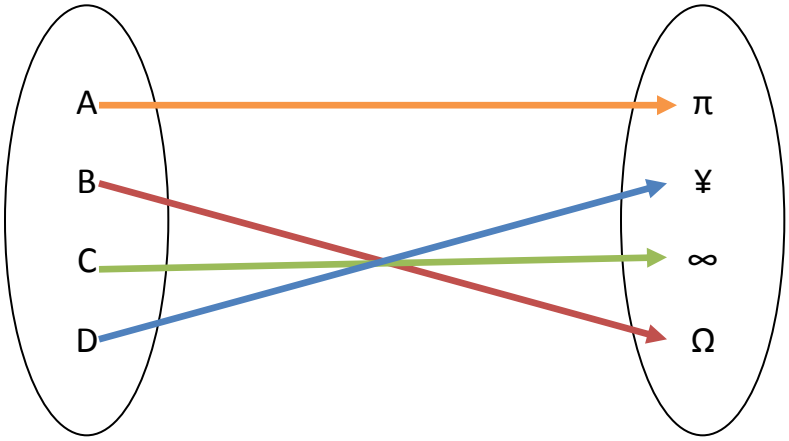


Figura. 1.11 Función Inyectiva.

Es *determinista* ya que para cada entrada siempre devolverá el mismo valor de salida.

Son de un sólo sentido ya que podremos computar un resultado de manera sencilla, por el contrario la obtención de la entrada a partir del resultado será computacionalmente inviable (*Véase fig. 1.11*).

Se refiere como inviable al hecho de que existen funciones matemáticas de las cuales se desconoce una forma sencilla de obtener su inversa, lo cual no quiere decir que sea imposible la obtención del mensaje a partir del resultado, sin embargo encontrar su función inversa podría ser tarea de años. Esta característica matemática de las funciones hash las hacen útiles en protocolos criptográficos

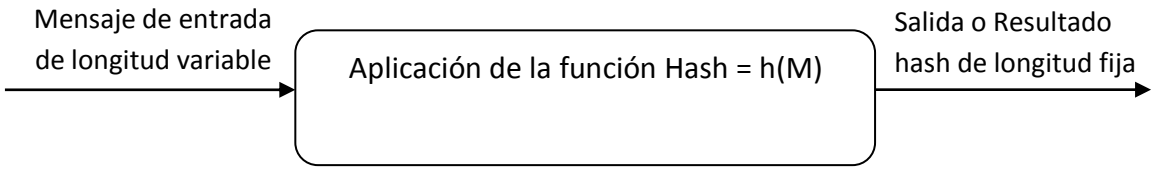


Figura 1.12 Esquema de funciones hash.

Al cifrar la información se dificulta el acceso a esta, sin embargo no es la única técnica con la cual se puede lograr este fin. Otra técnica conocida y la cual se ha popularizado es la esteganografía la cual dificulta el acceso a la información ocultándola. A veces estas técnicas se unen y la información aparte de cifrarse se oculta.

2.6. Esteganografía.

La esteganografía es una técnica con la cual se logra ocultar un archivo dentro de otro. La palabra esteganografía viene de la palabra griega *steganos* que significa oculto y *graphos* escritura. Cabe hacer la aclaración de que oculto no es lo mismo que cifrado. En este caso el archivo que se desea proteger sólo se oculta.

Se logra ocultar la información utilizando dos archivos: el primero que contiene la información y el segundo que servirá para ocultar el primer archivo.

La técnica consiste en modificar la estructura interna del segundo archivo, aprovechando que existen segmentos en la estructura que pueden ser modificados sin que los cambios sean perceptibles. Será en estos segmentos donde se oculte el primer archivo.

Uno de los métodos más comunes para ocultar información dentro de una imagen es el método de “sustitución del bit menos significativo” –LSB por sus siglas en ingles LeastSignificant Bit-. Este método consiste en guardar el mensaje que se desea ocultar en los bits menos significativos de cada uno de los tres bytes que se utilizan para definir un color en cada pixel.

Usando un modelo RGB –por sus siglas en ingles Red Green Blue- veremos que el primer byte define el color rojo, el segundo el color verde y el tercero el color azul cada color va desde 00000000 hasta el 11111111, teniendo que el cero indicara que no participa en la mezcla, a medida de que este valor aumenta se entenderá que aporta mayor cantidad de intensidad. Al combinar los tres obtendremos diferentes colores para un pixel.

Por ejemplo para representar el color amarillo necesitaremos que el valor del byte que representa la intensidad de rojo sea doscientos cincuenta y cinco, la del verde doscientos cincuenta y cinco y la del azul cero. (*Véase fig. 1.13).*

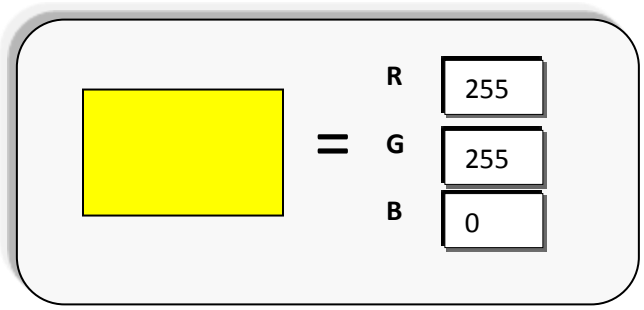


Figura 1.13 Representación del color amarillo en el modelo RGB.

Al guardar el mensaje cada byte que conforma el pixel se verá alterado, teniendo en cuenta que el bit que se modifique tendrá que ser el que contenga el valor menos significativo (*Véase tabla. 1.3).*

Tabla 1.3 Alteración del bit menos significativo.

Decimal	Binario	Bit Menos Significativo.
255	11111111	11111110
255	11111111	11111110
0	00000000	00000001

Una vez que se han hecho los cambios en el bit menos significativo obtenemos la alteración del color, la cual no es perceptible al ojo humano. (*Véase fig. 1.14).* Es por ello que funciona este método para ocultar información, además es imperceptible ya que el tamaño de la imagen no se altera ni tampoco su peso.

Figura 1.14 Alteración del bit menos significativo en el color amarillo.

Esto ejemplifica que existen diferentes técnicas para proteger la información, sin embargo estas técnicas también pueden ser utilizadas con un fin malicioso por ejemplo: la distribución de pornografía, esconder evidencia de un caso entre otros.

2.7 Seguridad, Criptografía y Cómputo Forense.

Se ha visto que para poder brindar un servicio de seguridad uno de los mecanismos más usados es la criptografía, sin embargo este mecanismo también lo encontramos implementado para perjudicar la seguridad de algún sistema o para evitar que se pueda culpar a alguien de alguna actividad ilícita. Por ello el cómputo forense ha tenido que irse actualizando tan rápido como estas prácticas lo hacen.

Las técnicas y métodos utilizados para atacar un sistema se encuentran en continuo desarrollo, podemos encontrar diferentes tipos de atacantes desde los que sólo se dedican a probar herramientas sin tener mayores conocimientos, hasta aquellos que poseen conocimientos profundos en redes, sistemas operativos, algoritmos de seguridad, vulnerabilidades en sistemas computacionales, metodologías de ataques… y no sólo eso sino que se preocupan por borrar o eliminar todo tipo de evidencia que pueda revelar su identidad y/o el procedimiento que usó para atacar el sistema. Esto lo logran destruyendo el dispositivo que las contiene, ocultando la evidencia, cifrándola o falsificándola.

Este tipo de atacantes son los que representan un verdadero reto cuando se trata de hacer una investigación forense. Usan herramientas de seguridad con el fin de mantener a salvo la evidencia que pudiera culparlos, es así como encontramos atacantes que mantienen archivos, carpetas o todo el disco cifrado usando contraseñas fuertes por lo que aunque el analista forense obtenga la imagen de su disco no podrá ver ningún dato en un formato entendible.

En estos casos se puede intentar la búsqueda de la contraseña por medio de fuerza bruta, ataques de diccionario o buscando un patrón en el uso de contraseñas del atacante, pero si no se tiene éxito lo más recomendable es continuar buscando información en otras fuentes. Ya que aún la ley no puede obligar a nadie a revelar su contraseña.

Las técnicas que utilizan los atacantes para proteger la información que los pueda incriminar son muy variadas desde el cifrado y la esteganografía hasta la destrucción física, como puede ser, la perforación del disco duro o la quema del equipo de cómputo.

Estos atacantes buscan siempre borrar las huellas que ha dejado su ataque, en el caso de la computadora que fue su víctima y dé la que les sirvió como medio, buscan hacer el borrado de bitácoras, archivos que hayan creado e instalaciones que hayan necesitado, esto lo pueden hacer una vez que han logrado su cometido o bien hacen la instalación de software para mantener censadas los equipos y hacer el borrado cuando creen que corren riesgo o bien al perder el control sobre ellas.

Por ejemplo: Cuando un equipo está censado las computadoras están programadas para hacer el borrado de evidencias en cuanto pierden la conexión por internet; lo cual asegura la eliminación de evidencia aunque el atacante ya no tenga el control sobre el equipo.

Y en los equipos que les sirvieron para guardar la información y dirigir el ataque, encontramos que una de las formas más comunes de destruir la evidencia es dañando los dispositivos físicamente, -golpearlos, perforarlos, quemarlos, echarlos al agua- o bien la sobre-escritura de los mismos.

Cualquiera que sea el escenario el analistas forenses tendrán que estar preparado, actuar con prontitud teniendo como prioridad la recuperación de toda la evidencia posible sin alterar su integridad.

Es por eso que es tan importante el nivel de conocimiento en los sistemas operativos: cómo funcionan, que información almacenan, que sistemas de archivos utilizan, que tipos de registros podemos encontrar, cómo se comportan sus partes mecánicas, y hasta un poco de física básica.

Por ejemplo: si la evidencia se encuentra sumergida en agua se tendrá que intuir que al contacto con el aire se iniciará un proceso de oxidación –al contacto

del metal con el aire-, por lo que para transportarla al laboratorio se mantendrá sumergida en agua, de esta manera lograremos conservar su integridad y probablemente la recuperación de evidencia sea más factible.

Ser cautelosos en la preservación y recuperación de evidencia es necesario tanto para el resultado exitoso de la investigación como para la protección legal del analista forense. Si en algún momento de la investigación se pierde la integridad de la evidencia se dudará del profesionalismo del analista forense culpándolo, por ejemplo, de complicidad y definitivamente la evidencia quedará anulada.

Atender un delito informático conlleva acatar las leyes impuestas por el estado, es por ello que es recomendable que el analista forense se encuentre asesorado durante todo el proceso por un abogado especialista en delitos informáticos.

3. Dispositivos de Almacenamiento.

Un dispositivo de almacenamiento es aquel que puede guardar información de forma digital. Por ejemplo: una memoria USB, un CD, un DVD, un disco duro, etc.

Para realizar el almacenamiento de información se usan diferentes técnicas dependiendo del dispositivo que se utilice, cada uno posee un algoritmo y registros con los cuales realiza las actividades de: almacenamiento, recuperación, actualización y eliminación.

Es muy importante puntualizar que la evidencia de la investigación, motivo de esta tesis, se presentó en un disco duro por lo que se hará un énfasis especial en este dispositivo de almacenamiento.

Se describirá su funcionamiento para explicitar la recuperación de información, la obtención adicional de archivos que evidencien datos importantes como la fecha y hora de creación y modificación, los autores y todo registro que enriquezca la investigación.

3.1. Estructura física de los Discos Duros.

Dentro del análisis forense una fuente primordial de evidencia suele ser el disco duro por ser el principal dispositivo de almacenamiento que tenemos en una computadora.

Un disco duro es un conjunto de componentes electrónicos y mecánicos que hace posible el almacenamiento y recuperación de información. La estructura física de los discos es similar sin importar su capacidad, velocidad, modelo o marca. Puede variar el tamaño, el peso, pero la estructura se conserva lo mismo que el funcionamiento.

El disco duro se encuentra formado por:

- Un gabinete de alta resistencia hecho de aluminio o metal sólido cerrado al vacio, que contiene las partes del disco duro.
- Una tarjeta de circuito electrónico de control que incluye una interfaz con la computadora.
- Un chip utilizado como memoria cache.
- Bobinas.
- Un bloque de brazos sujetos: en uno de sus extremos a un eje y en el otro extremo se encuentra una cabeza de lectura y escritura.

- Uno o varios discos o platillos hechos de una aleación de aluminio o bien los más modernos construidos de vidrio y cerámica, que giran sobre un eje central.
- Preamplificadores
- Conexiones de alimentación eléctrica -IDE ATA o SCOSI-.
- Una conexión del bus.
- Un bloque de configuración de jumpers.
- Un motor.
- Una bolsa de gel que evita la humedad interna del disco y se encuentra entre el disco y el gabinete.

Todas estas partes conforman e interactúan en un disco duro. La *fig.1.15* muestra la parte interna del disco duro, en específico se señala la ubicación del bloque de brazos, el motor, los ejes y los discos o platillos que giran sobre un eje.

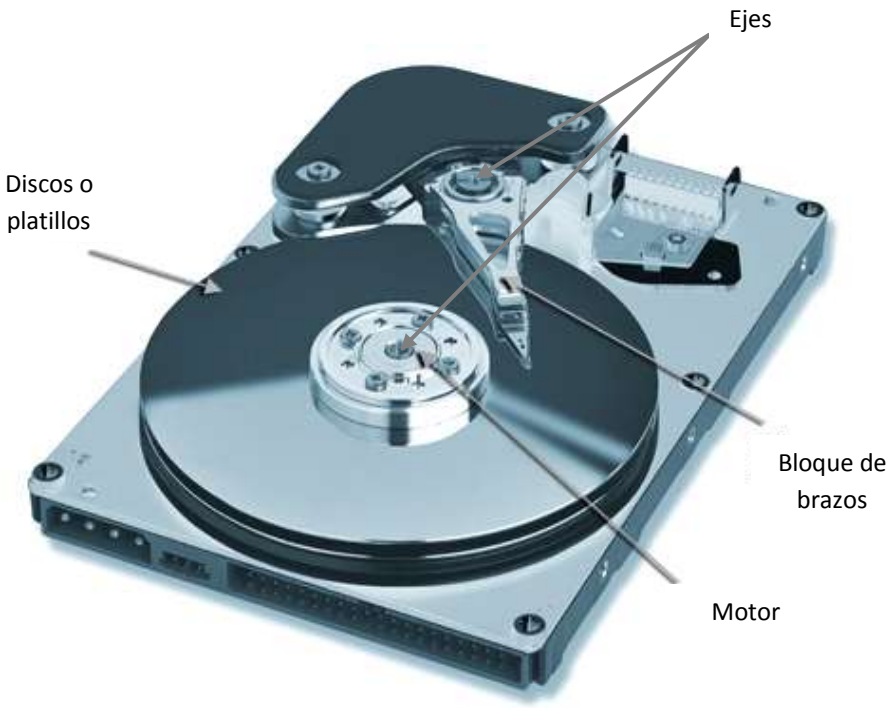


Figura 1.15 Estructura Física de un Disco Duro.

Al iniciar el funcionamiento del disco duro las bobinas hacen mover los ejes. El eje central donde se encuentran montados los discos puede girar a una velocidad de 7200, 9000, 10 000 y hasta 15 000 revoluciones por minuto. El otro eje es el encargado de mover el bloque de brazos, donde se encuentran las cabezas encargadas de la lectura y la escritura.

Mientras no esté en funcionamiento el disco duro, el bloque de brazos se encuentra descansando en uno de los extremos y al entrar en funcionamiento, el bloque se mueve desde la parte externa a la parte interna de los discos en busca de la información requerida, los brazos se mueven en conjunto es decir, todos al mismo tiempo y en la misma dirección.

Cuando se desea leer o escribir en el disco se mueve el bloque de brazos y se giran los discos hasta encontrar la posición a la cual se desea acceder.

Los discos o platillos cuentan común recubrimiento magnético que es la capa en donde residen los datos. Los discos se encuentran apilados con un pequeño espacio de separación entre ellos; cada disco puede leerse y escribirse por ambas caras, a cada cara se le llama plato.

Las cabezas de cada uno de los brazos se encuentran a una distancia de tres millonésimas de milímetro del plato por lo que la lectura y escritura se hace por magnetismo

El disco duro recibe instrucciones de la tarjeta madre por medio de un cable de bus -IDE, ATA o SCOSI-, que se encuentra conectado de la tarjeta madre a la tarjeta de circuito del disco, esta última manda las instrucciones a la cabeza por medio de un filamento, la cabeza hace la lectura o escritura correspondiente y es así como se encuentra la ubicación dentro de los discos o platillos.

El grupo de jumpers, que se encuentran ubicados entre los conectores de alimentación del disco, se utilizan para conectar más de un disco duro a una computadora e indicar la jerarquía entre ellos. La diferencia será que al iniciar la computadora arrancará el sistema que se encuentre en el disco de mayor

jerarquía -disco principal-, mientras que el de menor jerarquía -disco esclavo- sólo servirá de almacenamiento.

Es importante saber que existen diferentes tipos de conexiones para los discos duros -IDE, SATA, SCOSI- ya que al buscar preservar la evidencia almacenada en ellos es necesario contar con las conexiones adecuadas y prever el espacio necesario para almacenar la información obtenida.

3.2. Estructura lógica.

Así como la estructura física del disco duro facilita entender su funcionamiento mecánico, la estructura lógica facilitará el conocimiento sobre la organización y distribución de la información en este dispositivo.

Se ha creado una división lógica del disco duro para poder acceder a un punto específico dentro de éste. El disco duro se compone de varios discos o platillos, cada uno de estos discos tiene dos caras: una superior y una inferior, las cuales están divididas en una estructura lógica que emplea pistas, cilindros, sectores y clusters.

Las pistas son círculos concéntricos que dividen el disco y van desde la parte externa a la parte interna. El número de pistas está determinado por la capacidad del disco. (*Véase fig.1.16)*.

Los cilindros son usados para describir la misma pista sobre cada uno de los discos o platos que conforman el disco duro, es como una pista que atravesara a todos los platos que conforman el disco duro. (*Véase fig.1.16).*

Las pistas están divididas en sectores, como se ilustra en la fig. 1.16. El tamaño de cada sector no es fijo puede variar entre 512 bytes, 1024 bytes, 2048 bytes y hasta 4096 bytes aunque el estándar es 512 bytes. Antiguamente el

número de sectores por pista era fijo, lo cual desaprovechaba el espacio significativamente, ya que las pistas exteriores pueden almacenar más sectores que las interiores. El número de sectores también dependerá de la capacidad del disco duro.

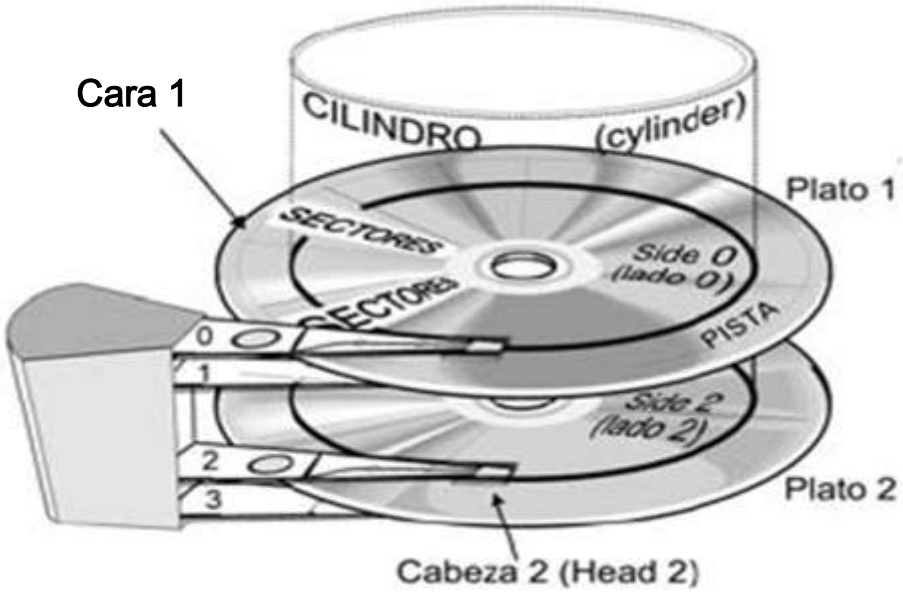


Figura 1.16 Estructura Lógica del Disco Duro.

Los clusters son agrupaciones de varios sectores ubicados en una misma pista, pueden tener 1, 2, 4, 8 o más sectores por lo cual su capacidad puede ser de 512 bytes, 1024 bytes, 2048 bytes o más. Un cluster es la unidad lógica más pequeña de almacenamiento en un disco. Al ser almacenados los archivos estos pueden ocupar uno o más clusters.

La cantidad de sectores que se asignen para formar un cluster dependerá del sistema de archivos. Dependiendo del sistema que los defina serán nombrados. Por ejemplo: en el sistema de archivos FAT a esta agrupación de sectores se les llama cluster, mientras que en sistema de archivos EXT3 se les llama bloques.

Las pistas y cilindros se numeran a partir del cero mientras que los sectores a partir del 1. Así el primer sector de un disco será el que se encuentra en la pista cero cilindro cero sector uno.

Los cluster son numerados secuencialmente a partir del 2 ya que el primer sector de todos los discos contiene el registro de arranque, en este primer sector se registra qué sistema operativo tiene instalado y qué tipo de sistema de archivos utiliza.

La información contenida en este sector –primer sector- es una fuente muy confiable para el analista forense, si lo que desea conocer es el tipo de sistema operativo del equipo.

Para poder leer o escribir en alguna sección del disco es necesario antes determinar la dirección del sector al cual se desea acceder para lo cual se establece una estructura lógica.

La estructura lógica del disco cambiará dependiendo del método de direccionamiento.

Si se utiliza el método de direccionamiento CHS (por sus siglas en Ingles “Cilinder-Head-Sector”), la estructura lógica deberá de conservar fijos el número de sectores por pista ya que los datos se localizaran en cualquier espacio del disco ubicando primero el cilindro posteriormente la cabeza y por ende la cara del disco y al final el sector.

Por ejemplo para un disco que utilizara el método de direccionamiento CHS, IBM establecía los siguientes valores que definen la estructura lógica de un disco duro de 8GB *(Véase tabla 1.4).*

Tabla 1.4 Especificación de cilindros, cabezas y sectores de IBM.

	Tamaño n del campo (bits)	Valor máximo teórico 2^n	Rango permitido	Total Utilizable
Cilindro	10	1024	0-1023	1024
Cabeza	8	256	0-255	256
Sector	6	64	1-63	63

En la tabla 1.4 podemos observar que el disco contiene diez cilindros que definen diez pistas en cada disco o plato y cada una de estas pistas está divida en seis sectores. Considerando que cada pista es de diferente tamaño dependiendo de qué tan cerca este del centro, se concluye que en las pistas exteriores se desperdiciará espacio ya que estas pistas podrían contener más sectores que las interiores. Lo que repercute directamente en la capacidad de almacenamiento.

Si se usa el método LBA (Direccionamiento lógico por bloques por sus siglas en Ingles Logical Block Addressing). La estructura lógica podrá definir diferente número de sectores por pista aprovechando totalmente el disco. La localización de los datos será por medio del número único que se le asigne a cada sector. Considerando el ejemplo anterior un disco duro con las mismas características, con este último método de direccionamiento, tendrá una mayor capacidad de almacenamiento.

3.3 Almacenamiento en discos duros.

El almacenamiento en discos duros se hace por medio de pulsos eléctricos, en donde a la existencia de un pulso eléctrico se le asigna un **1** y a la ausencia de este un **0**.

Por lo tanto el sistema numérico bajo el cual funciona la comunicación en la computadora es el sistema binario, que solo tiene dos símbolos –cero y uno- para la representación de cualquier dato. A cada uno de estos ceros y unos se les da el nombre de bit, el grupo de 8 bits corresponde a un byte.

Este sistema numérico es un sistema posicional al igual que el sistema decimal que es el que comúnmente utilizamos. Con posicional se entiende que el símbolo obtendrá valor según la posición que ocupe, así cada posición tendrá un valor determinado por las potencias de la base iniciando con 0, 1, 2, 3, iniciando de derecha a izquierda.

Por ejemplo:
Si tenemos el valor de 10111001.

Tabla. 1.5 Valores posicionales del sistema binario.

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor según la posición	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Número binario	1	0	1	1	1	0	0	1

Para conocer el valor de 10111001_2 en decimal se hace el siguiente cálculo:

$2^0 * 1 + 2^1 * 0 + 2^2 * 0 + 2^3 * 1 + 2^4 * 1 + 2^5 * 1 + 2^6 * 0 + 2^7 * 1$
$=128 + 32 + 16 + 8 + 1$
$=185$

De esta manera se obtiene que $10111001_2 = 185$ se considera el mismo valor representado en diferente base (en la base diez se omite el subíndice obedeciendo el principio matemático de economía).

En la tabla 1.5 se observa que cada columna tiene un valor, en este caso la columna de la derecha es la que tiene el valor menos significativo y la columna que se encuentra más a la izquierda tiene el valor más significativo.

Sin embargo en el lenguaje de la computadora este orden se puede invertir y entonces la columna con el valor más significativo será la que se encuentre más a la derecha y la columna con el valor menos significativo será aquel que se encuentre en la columna de la izquierda. Por lo que aunque tengamos la misma sucesión de símbolos el valor cambiara según el orden en el que establezcamos la posición más o menos significativa.

Dependiendo de qué valor se le dé a la columna de la derecha será como se le nombre a la organización, es decir si en la columna de la derecha está el más significativo se le nombrara “bigendian” y si este es el menos significativo será el “Little endian”.

La compañía Intel Pentium utiliza la organización Little endian, mientras que Sun SPARC y Motorola Power PC (Apple computer) utiliza la organización bigendian.

Los datos almacenados en sistema binario pueden presentarse ante el usuario en sistema hexadecimal para facilitar su lectura. A continuación se muestra en la tabla 1.6, los primero dieciséis valores binarios y su representación en hexadecimal y decimal.

Tabla 1.6 Primeros dieciséis valores decimales expresados en hexadecimal y binario.

Binario	Hexadecimal	Decimal
0	0	0
1	1	1
10	2	2
11	3	3
100	4	4
101	5	5
110	6	6
111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Cuando los datos se muestran en valores hexadecimales son precedidos por un '0x'.

En este sistema la base es dieciséis, la conversión de binario a hexadecimal será hará dividiendo la cifra en grupos de cuatro, se obtiene el valor decimal de cada grupo y se le asigna su valor correspondiente en hexadecimal. (*Véase tabla 1.6).*

Por lo que si tenemos el número binario: 011110101101 al hacer la conversión a hexadecimal obtendremos: 7AD. (*Véase tabla 1.7).*

Tabla 1.7 Conversión de binario a hexadecimal.

Número en binario 011110101101			
Valores posicionales en binario	$2^3\,2^2\,2^1\,2^0$	$2^3\,2^2\,2^1\,2^0$	$2^3\,2^2\,2^1\,2^0$
Dividido en grupos de cuatro	0 1 1 1	1 0 1 0	1 1 0 1
Valores en decimal	7	10	13
Conversión a hexadecimal	7	A	D

Para guardar una letra dentro del disco la técnica más usada es el código ASCII en donde a cada carácter se le asigna un valor numérico de 8 dígitos –un byte- Al tener ocho posiciones en sistema binario el total de combinaciones posibles es de 127. (*Véase tabla 1.8).*

La ventaja de esta técnica es que ocupa poco espacio para representar los caracteres optimizando el espacio en el disco duro.

Tabla 1.8 Valores del código ASCII.

DEC	HEX	Símbolo ASCII	DEC	HEX	Símbolo ASCII	DEC	HEX	Símbolo ASCII
0	00	NULL (Caracter nulo)	43	2B	+	86	56	V
1	01	SOH (Inicio de encabezado)	44	2C	,	87	57	W
2	02	STX (Inicio de texto)	45	2D	-	88	58	X
3	03	ETX (Final de texto)	46	2E	.	89	59	Y
4	04	EOT (Final de transmisión)	47	2F	/	90	5A	Z
5	05	ENQ (Enquiry)	48	30	0	91	5B	[
6	06	ACK (Acknowledgement)	49	31	1	92	5C	\
7	07	BEL (Timbre)	50	32	2	93	5D	]
8	08	BS (retroceso)	51	33	3	94	5E	^
9	09	HT (Tabulador horizontal)	52	34	4	95	5F	_
10	0A	LF (Salto de línea)	53	35	5	96	60	`
11	0B	VT (Tabulador vertical)	54	36	6	97	61	A
12	0C	FF (Form feed)	55	37	7	98	62	B
13	0D	CR (retorno de carro)	56	38	8	99	63	C
14	0E	SO (Shiftout)	57	39	9	100	64	D
15	0F	SI (Shift in)	58	3A	:	101	65	E
16	10	DEL (Data link escape)	59	3B	;	102	66	F
17	11	DC1 (Dispositivo de control 1)	60	3C	<	103	67	G
18	12	DC2 (Dispositivo de control 2)	61	3D	=	104	68	H
19	13	DC3 (Dispositivo de control 3)	62	3E	>	105	69	I
20	14	DC$ (Dispositivo de control 4)	63	3F	¿	106	6A	J
21	15	NAK (negative Acknowledgement)	64	40	@	107	6B	K
22	16	SYN (Syncronous idle)	65	41	A	108	6C	L
23	17	ETB (Final de transmisión de bloque)	66	42	B	109	6D	M
24	18	CAN (Cancelar)	67	43	C	110	6E	N
25	19	EM (end of mdium)	68	44	D	111	6F	O
26	1A	SUB (Sustitución)	69	45	E	112	70	P
27	1B	ESC (Escape)	70	46	F	113	71	Q
28	1C	FS (Separador de archivo)	71	47	G	114	72	R
29	1D	GS (Separador de grupo)	72	48	H	115	73	S
30	1E	RS (Record separator)	73	49	I	116	74	T
31	1F	US (Separador de unidad)	74	4A	J	117	75	U
32	20	Espacio	75	4B	K	118	76	V
33	21	!	76	4C	L	119	77	W
34	22	“	77	4D	M	120	78	X
35	23	#	78	4E	N	121	79	Y
36	24	$	79	4F	O	122	7A	Z
37	25	%	80	50	P	123	7B	{
38	26	&	81	51	Q	124	7C	|
39	27	‘	82	52	R	125	7D	}
40	28	(	83	53	S	126	7E	~
41	29	)	84	54	T	127	7F	DEL (Delete)
42	2A	*	85	55	U			

En la tabla 1.8 Se aprecia que no todos los símbolos utilizados tienen una representación numérica por ejemplo no existe la letra ñ, se encuentra limitado por el número de combinaciones posibles. Ante esta necesidad surgen otras técnicas como el Unicode de 96000 combinaciones asignables a un caracter, para lo cual requiere cuatro bytes como máximo para representar cada caracter.

El Unicode tiene tres formas de guardar los caracteres UTF-32 el cual ocupa 4bytes UTF-16 que requiere como máximo de espacio 2 bytes y UTF-8 el cual requiere 1,2 o 4 bytes. Tanto el UTF-16 como el UTF-8 varían en el número de bytes que utilizan para presentar un caracter esto lo hacen con la finalidad de optimizar el espacio en el disco, sin embargo usar varios tamaños dificulta el procesamiento.

El método más utilizado es el UTF-8 porque disminuye la pérdida de espacio, en este método se usa solo un byte para cada uno de los caracteres que contiene la tabla ASCII.

Para ver como son guardados los caracteres en un archivo dentro del disco duro, se creará un archivo cuyo contenido sea el nombre Esther Selene Morales (Esther espacio Selene espacio espacio Morales) y se abrirá con una herramienta llamada xxd de Linux la cual permite ver el contenido del archivo en un formato hexadecimal.

A continuación se muestra la imagen con el resultado que se obtiene al abrir con xxd el archivo creado. (*Véase fig. 1.17).*

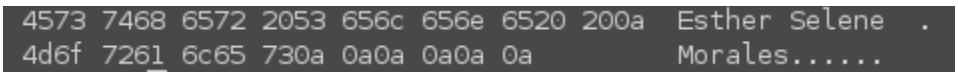


Figura 1.17. Archivo abierto con la herramienta xxd.

Considerando los valores de la *fig. 1.17* “4573 7469…” en correspondencia con la tabla del código ASCII (*Véase tabla 1.8.)* El número 45 que es el primer byte corresponde a la letra E, el 73 a la letra s, el 74 a la letra t el 69 a la letras e y

así sucesivamente. El número 20 corresponde a un espacio y el 0 señala el término de la línea. La razón de que aparezcan varios 0a al final de la palabra Morales es porque dentro del archivo se dieron seis enters.

Esta es la forma en que se visualiza la información al realizar un análisis forense, así se almacena la información en cada uno de los sectores del disco, esto da la opción de ver el contenido de archivos sin contar con la aplicación de creación.

4. Sistemas Operativos.

La estructura lógica, métodos de direccionamiento, y técnicas de almacenamiento son establecidas por los sistemas operativos.

Los sistemas operativos son programas que juegan un papel muy importante dentro de la computadora. Sin ellos sólo tendríamos un montón de fierro inútil. Una vez que se instalan los sistemas operativos, la computadora almacena, procesa y recupera información, muestra documentos, permite que el usuario navegue en internet, visualice videos, reproduzca sonido etc.

Los sistemas operativos son el programa fundamental que controla los recursos de la computadora, son la base para que se desarrollen otros programas.

Un sistema operativo moderno contempla el control de los procesadores, memoria RAM, discos duros, interfaces de red, impresoras, ratones y demás recursos de la computadora. Por lo tanto un sistema operativo se vuelve un programa complejo que controla todos estos componentes para que se usen correctamente y de manera óptima.

El sistema operativo tiene dos funciones básicas: la primera es la *comunicación y control* con todos los diferentes dispositivos que conforman la

computadora, la segunda función es la *administración de los recursos,* que consiste en el reparto ordenado de los recursos -procesadores, memorias, periféricos, etc.- entre los diferentes programas que compiten por ellos. Estas dos funciones permiten mostrarle al usuario una interfaz cómoda de trabajo acorde a sus requerimientos.

Cuando el sistema operativo tiene más de un usuario la administración y protección no sólo del hardware (disco duros, procesadores, memoria RAM, etc.) sino también de la información (archivos, base de datos, etc.) es primordial, para lo cual lleve el registro de todas las actividades realizadas por los diferentes usuarios y el tipo de privilegios que posee cada uno, atiende sus solicitudes, resuelve conflictos provenientes de los diferentes programas y usuarios.

Para instalar un sistema operativo se crea una partición en el disco duro. Esta partición tendrá la estructura lógica definida por el sistema operativo y la capacidad de almacenamiento que el usuario determine en el momento de la instalación.

Dentro de un mismo disco duro se pueden crear más de una partición, es decir se puede instalar más de un sistema operativo y trabajar como si se tuvieran varios discos duros.

En el primer sector del disco se encuentra el registro de la ubicación de las diferentes particiones alojadas en el disco; especificando el sector de inicio, el número de sectores que ocupa y el tipo de sistema de archivos que utiliza. En este sector se pueden describir máximo 4 particiones. A este primer sector que contiene el registro de particiones se le conoce como Master Boot Record (MBR).

El MBR sólo abarca un sector de 512 bytes, para almacenar los datos de cada partición ocupará 16 bytes. La primera partición se encuentra en el byte 446 (1BE en hexadecimal), la segunda en el byte 462 (1CE en hexadecimal), la tercera en el byte 478 (1DE en hexadecimal) y la 4 en el byte 494 (1EE en hexadecimal) terminando el registro de esta última en el byte 510.

Los 512 bytes del MBR no permite el registro de más de cuatro particiones Si se quisiera tener más de cuatro particiones será necesario definir otro tipo de particiones llamadas lógicas las cuales se definirán en una partición especial denominada partición extendida, esta partición tendrá que formar parte de las cuatro particiones primarias posibles.

En esta partición extendida habrá una tabla de particiones, en la cual se podrán registrar dos particiones de las cuales una puede tener un sistema de archivos y la otra puede ser otra partición extendida que a su vez nos permita la instalación de otro sistema de archivos y otra partición extendida. Es importante mencionar que las particiones lógicas no son *bootables* es decir no puede arrancar un sistema operativo que se encuentre instalado en ellas por lo cual lo único que podemos instalar en este tipo de particiones son sistemas de archivos.

Anteriormente hemos mencionado que dentro de la tabla de particiones que se almacena en los primeros 512 bytes se utilizan 16 bytes para describir o registrar cada partición. A continuación veremos qué es y cómo se almacena en esos 16 bytes.

El byte cero nos dará información de si la partición está activa o no, es decir si está es *bootable*. De ser que la partición este activa tendrá el valor 80 de lo contrario tendrá el valor 00. El byte uno registra la cara del disco donde inicia la partición. Del byte dos al tres se tendrá el registro del sector y cilindro donde inicia la partición. En el byte cuatro se encontrará el tipo de partición. En el byte cinco se encontrará la cara del disco donde acaba la partición. Del byte seis a siete se encontrará el sector y cilindro donde termina la partición. Del byte ocho al once se encontrará el sector de inicio de la partición. Y por último del byte doce al dieciséis se tendrá el tamaño de la partición. (*Véase tabla 1.9).*

Tabla 1.9 Descripción del contenido de los dieciséis bytes que describen cada partición.

Inicio (Decimal)	Longitud en bites	Contenido
0	1	Estado de la partición 00 si no está activo y 80 si está activo
1	1	Cabeza donde la partición empieza
2	2	Sector y cilindro donde la partición empieza
4	1	Tipo de partición
5	1	Cabeza donde la partición acaba
6	2	Sector y cilindro donde la partición termina
8	4	Distancia en sectores de la partición de la tabla a el primer sector de la partición (sector de inicio)
12	4	Número de sectores en la partición (tamaño de la partición)

Se sabrá que el MBR acaba cuando encontremos dos bytes con el siguiente valor en hexadecimal: 55 AA

Para poder distinguir el tipo de sistema de archivos que contiene cada partición debemos conocer los valores que identifican a cada sistema. A continuación se muestra una tabla con los tipos de sistemas de archivos más comunes y su representación en hexadecimal. (*Véase tabla 1.10).*

Tabla 1.10 Tipos de sistema de archivos con su valor hexadecimal.

Valor hexadecimal	Tipo de sistema de archivo
01	FAT12
0E	FAT16
0C	FAT32
83	Linux Nativo
82	Linux Swap
A5	BSD/386
05	Partición Extendida
07	NTFS

4.1. Sistemas de archivos

Así como las particiones distribuyen en el disco duro los sistemas operativos para que puedan convivir en un mismo disco, los sistemas de archivos organizan la información para que esta pueda ser almacenada, modificada y recuperada.

Los sistemas de archivos surgen de la necesidad de conservar la información. Un sistema de archivo permite guardar la información de manera persistente, se puede apagar la computadora, es decir finalizar los procesos, con la seguridad de que la información quedó almacenada y disponible. Y sólo podrá ser eliminada cuando su usuario así lo desee.

Los archivos son presentados ante el usuario en una interfaz gráfica amigable donde se pueden visualizar los archivos ordenados en carpetas, sin embargo dentro del disco duro los archivos se encuentran almacenados de forma distinta.

Para poder almacenar los archivos se establece una estructura que define los parámetros necesarios para poder cumplir con las tareas solicitadas: acceder a la información, protegerla, asignarla a un usuario, asignarle un nombre, etc.

La estructura está compuesta por cinco capas: la capa física, la capa del sistema de archivos, la capa de datos, la capa de metadatos y la capa del nombre. En cada una de estas capas se almacenan datos que sirven para administrar todos los archivos almacenados en el disco duro. A continuación se describen cada una de estas capas.

a) **Capa Física** es el dispositivo físico donde se encuentra almacenado el archivo, en el caso de la computadora la capa física es el disco duro.

b) **Capa del sistema de archivos** se refiere a la partición que contiene al archivo.

c) **Capa de datos** es donde se guardan los datos del archivo es decir los bloques o clusters que contienen al archivo. Los bloques o cluster tienen un tamaño definido previamente por lo que es probable que para guardar un archivo, un solo cluster o bloque no sea suficiente, si el archivo rebasara el tamaño del cluster entonces se le asignará otro cluster hasta poder almacenar el archivo.

Los bloques o cluster que se le asignen a un archivo no necesariamente deben ser contiguos. Para poder identificar los bloques o clusters de un mismo archivo el sistema de archivos implementa algo parecido a un listado donde registra el archivo y el número de los bloques o clusters que le pertenecen.

Para poder almacenar un archivo el sistema operativo necesita saber que bloques o sectores tiene disponibles en el disco. Para poder determinar que un bloque o cluster del disco está disponible se utilizan dos valores: asignado y no asignado. El valor asignado indica que se trata de un bloque o cluster que almacena un archivo activo en el sistema. Mientras que el valor no asignado indica que es un cluster disponible para almacenar a un archivo.

Una vez que se ha encontrado un espacio disponible –que tenga el valor no asignado- se guardará ahí el archivo. Si el bloque o cluster no fuera suficiente para almacenar el archivo entonces se buscará otro bloque o cluster no asignado donde se pueda almacenar la parte restante del archivo.

La necesidad de buscar otro bloque o cluster donde guardar el resto de la información del archivo puede suceder también en el caso de que un archivo guardado previamente haya crecido y el espacio de un bloque o cluster le resulte insuficiente, es en este caso cuando es más probable que el archivo quede almacenado en bloques o clusters no contiguos.

Cuando un archivo es borrado del disco duro, se le cambia al bloque(s) o cluster(s) el valor de asignado por el de no asignado, la información queda intacta y el valor de no asignado permite que el bloque o cluster sea sobrescrito, por lo que el estado no asignado no siempre significa que el bloque o cluster se encuentre libre de información. Razón por la cual es posible recuperar archivos que los usuarios han borrado aunque no aparezcan visibles en la interfaz de usuario, ya que estos aún residen en el disco duro, sin embargo, también es posible que no sea tan fácil su recuperación porque ya estén sobre-escritos.

Es por esto que un analista forense examina todo el disco duro con herramientas que le permiten ver la información que se encuentra almacenada en cada bloque sin importar si estos contienen el estado de asignado o no asignado.

Si realmente se desea borrar un archivo del disco se emplean alguna de las siguientes técnicas: la sobre-escritura o wiping (limpieza), la magnetización o la destrucción controlada de medios.

La *sobre-escritura o wiping* consiste en sobre-escribir varias veces el espacio que contenía al archivo que se desea borrar, se recomienda que la sobre-escritura no se haga menos de siete veces ya que existen técnicas con las cuales se puede recuperar la información de un bloque o cluster aunque este haya sido sobre-escrito.

A continuación se muestra una tabla en la que se describen algunos métodos para realizar el borrado de medios mediante el uso de la técnica de sobre-escritura *(Véase tabla 1.11).*

Tabla 1.11 Métodos para el borrado seguro de datos.

Grado	Método	Descripción.	Nivel de seguridad
1	Escritura de Ceros (súper rápido)	Sobre- escritura del medio con un valor fijo (0x00) en cada tercer sector	Bajo
2	Escritura de Ceros (rápido)	Sobre-escritura del medio con un valor fijo (0x00) en cada sector	Bajo
3	Escritura de Ceros	Sobre-escritura de medio con un valor fijo (0x00) en toda el área del medio	Bajo
4	Escritura Random	Sobre-escritura del medio con valores aleatorios	Medio
5	Escritura de Random y ceros	Sobre-escribe el medio con valores aleatorios, lo vuele a sobre-escribir con el valor fijo (0x00), sobre-escribe con valores aleatorios y termina sobre-escribiendo con el valor fijo (0x00).	Medio
6	US Navy, NAVSO P-5239-26 – MFM	Estándar de la Armada estadounidense (US Navy) NAVSO P-5239-26 para discos codificados con MFM (Modified Frequency Modulation). El método consiste en la escritura de un valor fijo (0xffffffff) sobre el medio, después un valor fijo (0xbfffffff), y finalmente una serie de valores aleatorios. El área de datos se lee para verificar la sobre-escritura.	Medio
7	US Navy, NAVSO P-5239-26 – RLL	Estándar de la Armada estadounidense (US Navy) NAVSO P-5239-26 para discos codificados con RLL (Run Length Limited). Este método aplica la escritura de un valor fijo (0xffffffff) sobre el medio, un valor fijo (0x27ffffff), y finaliza con valores aleatorios. El área de datos se lee para verificar la sobre-escritura. El método es aplicable a discos duros y soportes ópticos como el CD, DVD o el disco BlueRay.	Medio
8	Bit Toggle	Sobre-escritura de toda la zona de datos cuatro veces, primero con el valor (0x00), sigue con el valor (0xff), luego (0x00) y finaliza con (0xff).	Medio
9	Random Random Cero	Sobre-escritura del medio dos veces con valores aleatorios, una vez más con un valor fijo (0x00). Vuelve a sobre-escribir dos veces con valores aleatorios y una última vez con ceros.	Medio
10	Departamento de Defensa E.U.A (DoD 5220.22-M)	Este método de borrado fue introducido por el Departamento de Defensa de los E.U.A (Pentágono) y es conocido como "DoD5220.22-M". El método consiste en la sobre-escritura del medio con un valor fijo determinado una vez (por ejemplo 0x00), seguidamente se escribe su valor complementario (0xff) una vez, y finalmente se repasa con valores aleatorios una vez. El disco se verifica para comprobar la escritura correcta de los valores.	Medio

11	Fuerza aérea de los E.U.A, AFSSI5020	Estándar de las Fuerzas Aéreas de los E.U.A. (US Air Force) AFSSI5020. Este método de borrado primero sobre-escribe el soporte con un valor fijo (0x00), después otro valor fijo (0xff), y finalmente un valor aleatorio constante. Se comprueba al menos un 10% del disco para verificar la sobre-escritura.	Medio
12	Organización del Atlántico Norte OTAN estandar	Estándar de borrado de la OTAN (North Atlantic Treaty Organization). Sobre-escribe el medio siete veces. Las primeras seis veces son de sobre-escritura con valores fijos alternativos entre cada vez (0x00) y (0xff). La séptima pasada sobre-escribe con un valor aleatorio.	Alto
13	Peter Gutmann Borrado Seguro	El método fue creado por Peter Gutmann en 1996. Probablemente sea el método de borrado de datos más seguro que existe sin combinación con otros métodos. La sobre-escritura del medio se realiza grabando valores aleatorios cuatro veces sobre cada sector. Seguidamente se sobre-escribirá todo el soporte con valores pseudo aleatorios sobre cada sector durante veintisiete veces. Para terminar, se escribirán valores aleatorios durante cuatro veces sobre cada sector. En total, se realizan treinta y cinco veces de sobre-escritura.	Alto
14	Departamento de Defensa de los E.U.A (DoD 5220.22-M) + Método Gutmann	Método de alta seguridad consistente en sobre-escribir 35 veces, complementables con iteraciones de Mersenne, para agilizar los procesos de borrado seguro mediante la generación de números pseudo aleatorios.	Muy alto

La *magnetización* este proceso se hace acercando al disco duro un imán de gran potencia.

La *destrucción controlada de medios*, este es el método que se considera más seguro para borrar archivos. Para poder hacer la destrucción de los medios es necesario contar con ambientes especializados. Algunas de las técnicas para lograr la destrucción del medio son: la trituración, la incineración, la aplicación de químicos como son el ácido, la elevación de temperatura, la aplicación de altos voltajes por encima de las especificaciones del fabricante entre otras.

Cuando ocupamos más de un bloque o cluster para almacenar un archivo es probable que el último utilizado no se haya llenado por

completo, a este espacio sobrante se le conoce como “slackspace”. Este espacio queda reservado por si el archivo crece, de no ser así, es un espacio que se desperdicia.

Es posible que el “slackspace” de un archivo sobre-escrito contenga información de un archivo anterior. Esto dependerá de la diferencia de espacio utilizado por el primer archivo con relación al archivo que se sobre-escribe y del sistema operativo que se utilice en esa partición.

Por ejemplo Windows al no llenar un bloque o cluster, asigna un valor nulo al final del último sector que se ocupó, para identificar en donde terminan los datos del archivo. De esta forma en el “slackspace” encontraremos información del archivo que se contenía anteriormente –si es que se tratara de un bloque o cluster sobre-escrito-.

En el caso de Unix este sobre-escribe el espacio no utilizado en el bloque o cluster asignándole bytes nulos. Por lo cual en este caso no podremos encontrar información del archivo que se almacenaba anteriormente, al menos que se utilicen técnicas especializadas.

d) **Capa de metadatos.** En esta capa se encuentra una estructura con los valores que describen al archivo. El prefijo “meta” significa sobre datos, por lo que la estructura de metadatos será la estructura que contenga datos sobre los datos.

En esta estructura se encuentra información de la ubicación del archivo dentro del sistema de archivos, proporcionándole al sistema el número del bloque o cluster asignado al archivo, tal como lo hacían los catálogos de las bibliotecas que tenían que ser consultados si se quería encontrar un libro. Es en esta estructura donde se encuentra la información de todos los bloques o clusters que componen un archivo (a manera de listado), es decir se establece una correlación bloque o

cluster y archivo. De ahí que no sea necesario que los bloques o clusters que contienen al archivo sean contiguos.

En esta estructura también se encuentra: la fecha de creación, acceso y modificación; los mecanismos de seguridad, el tamaño, el tipo de archivo, los punteros a los datos y el (los) propietario y en algunos sistemas también el nombre.

La información que se refiere a los mecanismos de seguridad sirve para controlar el acceso de los usuarios al archivo ya sea para la lectura, escritura, ejecución o eliminación, dando la opción de otorgar diferentes permisos dependiendo del usuario que desee acceder al archivo.

Todos los sistemas de archivos tiene una estructura que es usada para describir al archivo, cada sistema de archivos nombra a esta estructura de diferente manera. Por ejemplo.

- En UNIX/ Linux se le llama inodo
- En el sistema NTFS se le llama Tabla maestra de archivos
- En el sistema FAT se le llama directorio de entrada

Esta capa también se encuentra algún método que sirve para hacer referencia al espacio que contiene almacenado dicho archivo, le dice al sistema como acceder a los bloques o clusters de un mismo archivo.

Esta estructura generalmente se encuentra oculta para los usuarios. Para un analista forense la información contenida en esta estructura es muy útil.

e) Capa del nombre. Dependiendo del sistema de archivos usado, será el lugar donde se guarde el nombre del archivo, puede ser dentro de la estructura de los metadatos o en una estructura aparte. Por ejemplo en el sistema de archivos FAT el nombre del archivo se guarda en la capa de los metadatos, mientras que en los sistemas de archivos utilizados por UNIX se guardan en otra estructura.

En esta capa se guarda el nombre del archivo, los directorios padre que lo contienen y la dirección de la estructura de metadatos.

Las reglas para poder darle nombre a un archivo dependerán del sistema de archivos, existen algunos que permiten caracteres especiales y otro no, o bien los que hacen distinción entre mayúsculas y minúsculas. El sistema de archivos también definirá el espacio permitido para almacenar el nombre.

En el nombre se puede reconocer dos partes principales delimitadas por un punto, del lado derecho del punto se encuentra el nombre del archivo y del lado izquierdo del punto se encuentra la extensión.

La extensión algunas veces es utilizada por los programas para saber el tipo de tratamiento que se le dará al archivo. Por ejemplo los compiladores de C forzosamente necesitan que los archivos a ser compilados tengan la extensión *.c*. Comúnmente la extensión indica que formato tiene un archivo, sin embargo esta información no es totalmente confiable ya que la extensión es fácilmente modificable por el usuario.

Una manera confiable de reconocer el formato del archivo es a través de la consulta de un número que se conoce comúnmente como número mágico.

4.1.1. Número Mágico.

El número mágico también es conocido como firma del archivo. Se le denomina mágico ya que el significado de este valor no es perceptible, a menos que se tenga un conocimiento previo del significado de ese número.

El número mágico se encuentra en los primeros bytes del archivo, este número indica el formato del archivo. Para poder visualizar este número es necesario hacer uso de alguna herramienta que abra el archivo en hexadecimal.

Es necesario aclarar que no todos los archivos poseen una firma o número mágico con el cual se pueda determinar su formato, por ejemplo los archivos de texto plano como lo son los archivos HTML, XHTML, XML y archivos de código fuente no poseen un número mágico que los identifique.

A continuación se muestra una tabla con los números mágicos de los archivos más comunes (*Véase tabla1.12)*

Tabla.1.12 Descripción del tipo de archivo por su número mágico.

Formato de Archivo	Número Mágico	Valor ASCII
GIF	47 49 46 38 39 61 47 49 46 38 37 61	GIF89a GIF87a
PNG	89 50 4e 47	ëPNG
PDF	25 50 44 46	%PDF
Archivos comprimidos .zip	50 4b	PK
Documentos de Microsoft Office	Que inicie con D0 CF 11 E0	

En esta tabla podemos ver la asociación del formato de archivo con su respectivo número mágico y los valores correspondientes en código ASCII. El número mágico será el valor que encontremos al abrir el archivo en formato hexadecimal.

En la figura 1.18 se puede ver como identificar el número mágico de un archivo PDF una vez que se ha abierto con un editor hexadecimal. En este caso se uso el editor llamado HexEdit.[4]

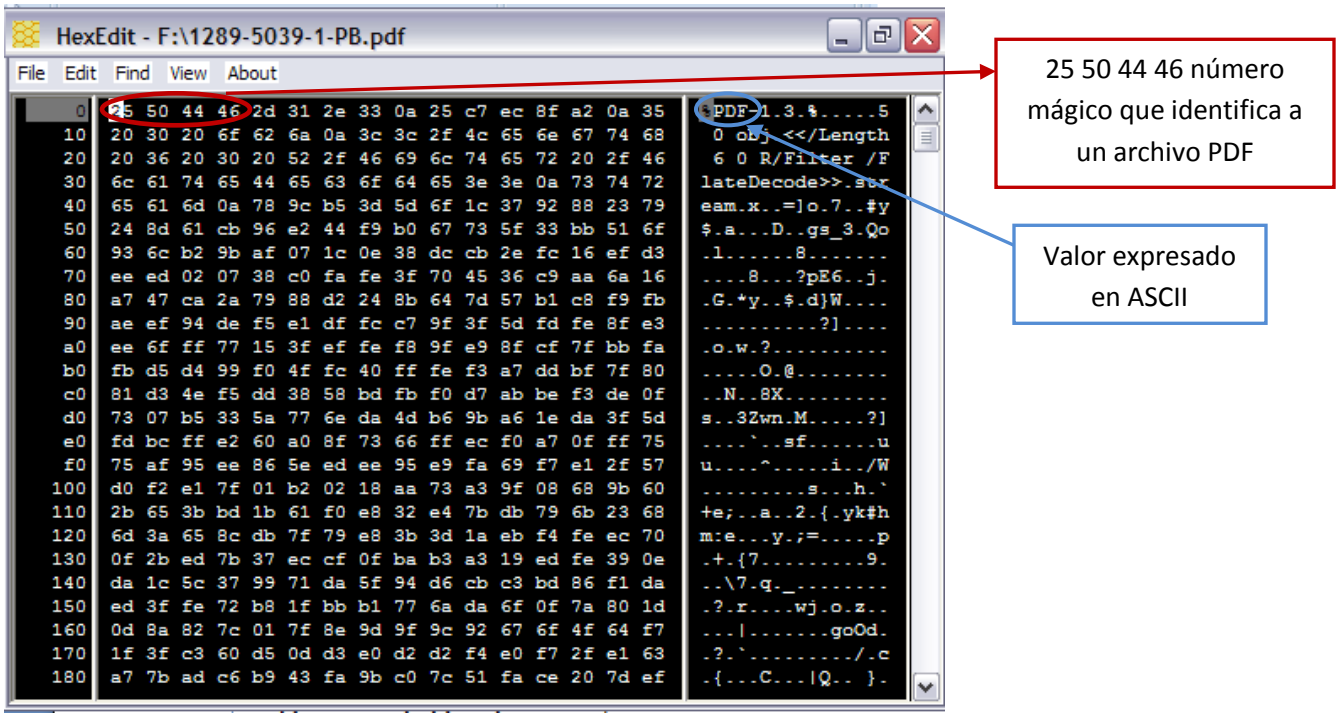


Figura.1.18. Identificación del número mágico de un archivo PDF abierto con un editor hexadecimal.

En este capítulo se han tratado temas necesarios para poder entender los objetivos y actividades realizadas durante una investigación cómputo forense.

El siguiente capítulo se enfocara completamente al área de cómputo forense, partiendo desde su origen, conociendo su desarrollo a través del tiempo, sus objetivos y las actividades que realiza para alcanzarlos, hasta las leyes con las que se cuenta actualmente para legislar tanto las actividades realizadas por el cómputo forense como los delitos en los que se ve involucrado algún dispositivo que almacena información digital.

[4]HexEdit v1.03 es un editor de texto libre.

Capítulo Segundo
Cómputo Forense.

En México como en otras partes del mundo cada vez se han registrado más delitos en los que se ve involucrado algún dispositivo de cómputo. Por lo cual se hace necesario contar con métodos que establezcan las formas en que debe tratarse este tipo de delitos; tanto en el ámbito de la investigación como en el campo legal.

Es el cómputo forense la ciencia que nace como garante de la justicia para resolver delitos donde la evidencia se encuentra almacenada en dispositivos de cómputo. Para poder lograr desempeñar esta actividad es necesario tener conocimientos tanto del dispositivo como de los procedimientos que se tienen que seguir para realizar una investigación forense y hacer la presentación de la evidencia.

1. Historia de la ciencia forense.

El cómputo forense tiene como raíz la ciencia forense, ciencia que es importante conocer ya que el cómputo forense comparte características esenciales con ésta. De esta manera se entenderá mejor su objetivo.

La palabra forense viene del Latín “forensis” que significa “para o delante del foro” [Diccionario de la lengua española, 2001]. Esto viene desde la época de los romanos donde una infracción penal significaba presentar el caso delante de un grupo de individuos dentro de un foro.

Todas las personas acusadas dentro del crimen y el acusador tenían que dar un discurso, narrando la parte de la historia que ellos vivieron. La persona con el mejor argumento y mayor habilidad verbal para presentar su discurso forense seria la persona que ganaría el caso.

Este origen es la fuente de los dos usos más comunes para la palabra forense: como la forma legal de la evidencia y como una presentación pública.

Desde hace mucho años se ha practicado la ciencia forense, uno de los ejemplos más antiguos que se conoce es el análisis que se practicó al cuerpo de Julio Cesar en el año 44 a.C. Después de haber sido asesinado, se encontró que Julio Cesar había sido apuñalado 23 veces pero solo la segunda herida hecha en el pecho había sido fatal.

Desde entonces esta ciencia se ha desarrollado logrando grandes avances como:

- El primer estudio de huellas digitales registrado hecho por Francis Galton (1822-1911)
- El descubrimiento de los grupos sanguíneos Lattes Leona (A, B, AB y O) (1887-1954)

- La comparación de balas para la resolución de casos Calvin Goddard (1891-1955)
- El desarrollo de las características esenciales para la el examen de documentos Albert Osborn (1858-1946)
- El desarrollo de los 10 puntos para determinar un Modus Operandi de un delincuente usado en diferentes escenas del crimen. (1883 L.W Atcherley)
- Establecimiento de un laboratorio del FBI para proporcionar los servicios forenses a todos los agentes de campo y otras autoridades de la ley a través del país. (1934)

Revisando estos eventos históricos se puede observar como a través de los años las personas van creando patrones de confianza en fuentes de información recuperada y analizada por la ciencia forense.

Cada vez se busca obtener más datos que ayuden a reconstruir los hechos para tener una certeza de lo sucedido, se desarrollan técnicas que se implementan en diferentes campos como la medicina, la odontología, la geología, en el estudio de documentos impresos, en datos digitales, en computación....

El hecho de que se busquen evidencias en los dispositivos de cómputo se debe a que en ellos se almacena información. El usuario de: una computadora, una laptop, alguna tableta electrónica, un celular, una memoria USB, etc., guarda información valiosa en estos dispositivos, los cuales son altamente vulnerables a un ataque e incluso se vuelven herramientas de delitos de cómputo.

La obtención de información a partir de los datos digitales almacenados en cualquier dispositivo de cómputo será la tarea principal a realizar por el cómputo forense.

A continuación se muestran los hechos más relevantes que marcaron el inicio del cómputo forense.

Esta ciencia nace en los años 70's, década en la que la computadora se vuelve personal, la venta de ésta se hace a gran escala y se crea la primera red de computadoras. Esto hechos revolucionan el campo de la comunicación a tal magnitud que fue imposible dimensionar el crecimiento y sus consecuencias, por lo que la presencia del cómputo forense fue inminente.

- En los 70's
    - Se encontraron los primeros casos de fraude financiero en donde se venían envueltos equipos de cómputo.
    - En Florida en el "Computer Crimes Act" se reconocen crímenes de sistemas informáticos como el sabotaje, copyright, modificación de datos y ataques similares (1978)

- En los 80's
    - Se hace el mayor desarrollo en esta área ya que las computadoras personales se convirtieron en una opción viable para los consumidores
    - Las cortes e investigadores financieros se dieron cuenta de que en algunos casos todos los registros y evidencias se encontraban sólo en las computadoras.
    - La Asociación de Examinadores de Fraudes certificados buscó capacitación en lo que más tarde se conociera como cómputo forense
    - El FBI crea el programa de medios magnéticos, mas tarde este se convierte en El equipo de Análisis Informático y Respuesta (CART) (1984)

- Acces Data- forma una empresa forense (1987)
- Creación de IACIS, la Asociación de Especialistas en Investigación Informática (1988)

- En los 90’s
  - Se establece la Organización Internacional en Evidencia Computacional (International Organization on Computer Evidence IOCE) (1993)
  - Se forma la Organización Internacional en Evidencia de Cómputo. (1995)
  - Se reconoce ampliamente que los funcionarios del orden público en todo el mundo necesitan estar preparados para adquirir evidencia de las computadoras (1997)
  - La interpol celebró un simposio de informática forense (1998)
  - El programa del FBI CART abordó 2000 casos individuales examinando 17 terabytes de datos. (1999)

- En la primera década del siglo XXI
  - Se pone en operación la Policía cibernética. La PFP (2001)
  - El número de casos del FBI CART continuó creciendo pasando de 17 terabytes analizados en 1999 a 782 terabytes analizados en sólo un año (2003).

- Se crea en México la Unidad de Investigación Cibernética[5]. (2007)

Como podemos ver mientras que en Estados Unidos de América específicamente Florida se reconoce los delitos informáticos desde 1978 en México no fue sino hasta el 17 de Mayo de 1999 que se considera necesario recurrir al derecho penal y se tipifican siete delitos informáticos. Es así como se publica en el Diario Oficial de la Federación en México, los nuevos delitos que protegen la información contenida en los sistemas y equipos de cómputo "Delitos informáticos". Y es hasta el 2007 que se crea una unidad de Investigación cibernética

Si comparamos a México con otros países la tipificación de delitos informáticos aún es nueva y existe muy poca gente que sabe de ellos o de las penas que estos tienen, aún se cree que en México no existe legislación para delitos informáticos. Sin embargo esto no nos exenta de que los padezcamos y causen daños.

Según estadísticas publicadas por Symantec en el 2011 ocho de cada diez adultos en México, usuarios de internet, han sido víctimas del cibercrimen[6]. Esto coloca a México en el tercer lugar mundial con más víctimas por crímenes cibernéticos sólo por debajo de China que cuenta con un 85% y Sudáfrica con un 84%.

[5]La policía cibernética de México tiene como función principal combatir la pornografía infantil vía internet. Además de esta atiende otros delitos principalmente aquellos que atentan contra las instituciones y la población vulnerable

[6] Cibercrimen empleado para definir actividades delictivas realizadas con ayuda de herramientas informáticas, esencialmente el internet.

2. Escena del crimen.

Cada vez es más frecuente ver o saber de personas que han sufrido algún daño por crímenes cibernéticos y es que el valor de la información muchas veces sobrepasa el valor del dispositivo que las contienen por lo que cada vez es más común que los delitos que se comentes sean por la obtención de información y no tanto por el robo del dispositivo.

La escena del crimen ha cambiado antes se podía apreciar la extracción del o de los objetos robados, y las evidencias que se podían encontrar eran: huellas dactilares, las armas o herramientas utilizadas para poder entrar de manera ilegal a la zona donde se encontraba su objetivo, testigos oculares. Si se había cometido algún asesinado se podía encontrar el arma homicida, las huellas del asesino, el cuerpo del asesinado entre otros. Y era a partir de estos elementos que se iniciaba la investigación *(Véase fig.2.1).*

Figura 2.1 Antigua escena del crimen.

Ahora en la escena del crimen es común encontrar algún dispositivo que guarde información digital que da evidencias contundentes y precisas que ayudan a esclarecer el crimen de una manera distinta a las técnicas utilizadas a partir de las evidencias descritas anteriormente. Cuando se trata de un crimen digital la

evidencia principal que se tiene es la información almacenada en los dispositivos involucrados *(Véase fig. 2.2)*.

Figura 2.2 Escena del crimen moderna.

La introducción de nuevas tecnologías ha cambiado la concepción del trabajo, entretenimiento, educación, política, comercio… inherente a esto cambian los entornos y por ende la renovación de las prácticas indebidas, teniendo como delitos más comunes: el acceso ilegal a sistemas, la intercepción ilegal de información, el robo y eliminación de información, interrupción de sistemas, distribución de pornografía infantil y fraude electrónico.

Ahora es necesario contar con personal especializado, métodos y legislación que ayude al tratamiento de este tipo de delitos a través de un proceso legal y una condena al que se encuentre culpable.

El analista forense es un personal especializado para desarrollar una investigación ante un delito digital con bases en el cómputo forense y aplicando la legislación correspondiente, contenida en el código penal federal.

3. Cómputo forense.

El cómputo forense nace como una disciplina auxiliar de la justicia moderna como garante de la verdad alrededor de la evidencia digital que sea presentada en un proceso legal.

Por ser esta ciencia relativamente joven aún existe la disputa entre algunos grupos lo consideran una técnica y tienen sus reservas para pensar en el cómputo forense como una ciencia. Sin embargo éste cuenta con las siguientes características que fundamentan el cómputo forense como una ciencia:

- La creación de teorías que tratan de explicar cómo funcionan las cosas.
- La comprobación de la teoría por métodos científicos comprobables.
- Empleo de herramientas y métodos científicos.

La ciencia forense digital ha sido definida por DFRWS[7] como “el uso de métodos derivados y comprobados científicamente para la preservación recolección, validación, análisis, interpretación, documentación y presentación de evidencia digital derivada de fuentes digitales, con el fin de facilitar o favorecer la reconstrucción de los hechos acontecidos en un delito, o ayudar a la anticipación de acciones no autorizadas perjudiciales para la planeación de operaciones” [DFRWS, Pág. 22].

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

[7] DFRWS (Digital Forensic Research Workshop) Organización dedicada a la puesta en común de conocimiento e ideas acerca de la investigación forense digital.

La definición más aceptada que defina al cómputo forense es: “El cómputo forense es la aplicación de técnicas científicas y analíticas a infraestructura de cómputo para preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal.”

Algunos autores hacen la distinción entre lo que es el forense digital y el cómputo forense, sin embargo en este trabajo se toma como dispositivo de cómputo no solo a una computadora de escritorio sino a todo aquel dispositivo que almacene datos de forma digital, por lo cual se tomará como sinónimo forense digital y cómputo forense.

El uso de esta ciencia ha ido en crecimiento debido a la gran variedad de dispositivos digitales que se han ido adoptando en las diferentes actividades de la vida diaria, y a que estos han sido utilizados para realizar actividades criminales, ya sea como el medio para realizar algún ataque o bien como el blanco de ataque.

Para poder atender cada uno de estos dispositivos y ofrecer un apoyo a la justicia, el cómputo forense se ha ido ramificando con el objetivo de especializarse y poder atender cada uno de los dispositivos que se pudieran encontrar en la escena del crimen. *(Véase fig.2.3).*

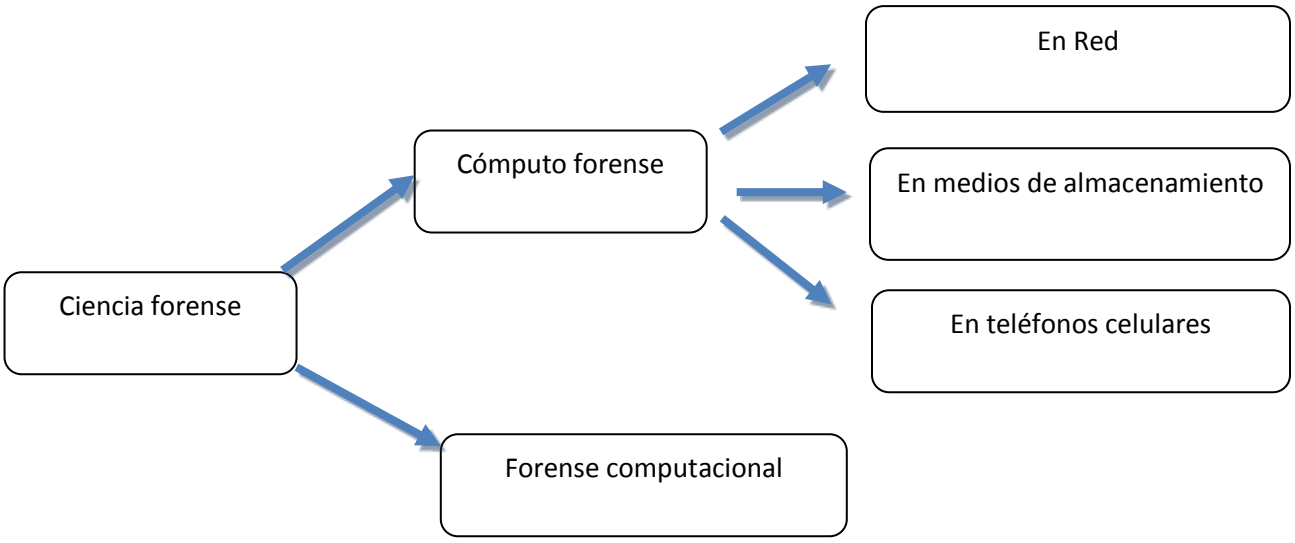


Figura 2.3 Ramificación de la ciencia forense.

En esta imagen se puede ver como el cómputo forense se divide en: cómputo forense en red, cómputo forense en medios de almacenamiento y cómputo forense en teléfonos celulares esta división es dependiendo del trato que se le tiende que dar a la evidencia encontrada en este tipo de dispositivos, ya sea para la recolección, análisis o presentación.

En la figura 2.3 se puede apreciar como una rama más de la ciencia forense el forense computacional. Esta ciencia es la encargada del desarrollo de algoritmos y software que ayuden al análisis forense de la evidencia digital.

3.1 Objetivos del Cómputo Forense.

El cómputo Forense tiene 3 objetivos principales que son:

- La identificación de los daños causados por los intrusos o criminales.
- La persecución y enjuiciamiento de los criminales.
- Proponer medidas para prevenir casos similares.

Se desglosará cada uno de los objetivos que se deben cumplir en una investigación de cómputo forense, enfocando las actividades a realizar para cumplir con el objetivo.

- ***Identificación de los daños causados por los intrusos o criminales.***

  Aquí englobamos actividades que ayudan a dimensionar el daño causado por las acciones del intruso en el sistema. Etas son: La recuperación de archivos, El análisis del sistema para identificar las actividades realizadas por el intruso, La identificación de robo de información, Análisis de malware, etc.

- ***La persecución y enjuiciamiento de los criminales.***

  Para lograr la persecución y enjuiciamiento de algún criminal es necesario analizar la información con el fin de encontrar pistas y pruebas que ayuden en el procedimiento legal. Para cumplir este objetivo se deben incluir todas las actividades que proporcionen la adecuada preservación de las evidencia. La validación de la integridad de la evidencia será lo que se valide en un procedimiento legal para decidir si puede ser presentada ante una corte legal

- ***Proponer medidas para prevenir casos similares.***

  Después de haber realizado el análisis y haber podido contestar el ¿Quién? ¿Cómo? ¿Cuándo? ¿Dónde? ¿Por qué? Se puede apoyar a las organizaciones proponiendo para que estas tengan una adecuada Administración de la Seguridad Informática.

Para lograr estos tres objetivos el cómputo forense cuenta con dos principios: el principio de Heinsenberg y el principio de Locard, así como metodologías y buenas prácticas que ayudan a conducir una investigación forense al éxito.

3.2 Principio de Heinsenberg.

Este principio se aplica en la etapa de preservación de la evidencia, cuando se desea mantener la evidencia integra. Al aplicar este principio dentro de una investigación de cómputo forense se puede determinar que será imposible preservar un sistema tal y como se encontraba en el momento del incidente. El principio dice así:

“Es imposible conocer simultáneamente la posición y velocidad del electrón y por lo tanto es imposible determinar su trayectoria. Cuando mayor sea la exactitud

con la que se conozca la posición, mayor será el error de la velocidad, y viceversa…"

Dentro del cómputo forense al querer preservar el sistema se encuentra que al examinar o coleccionar alguna parte del sistema irremediablemente se verán alterados otros componentes. Por lo que es imposible capturar un sistema completo en un punto del tiempo, y los cambios serán inevitables.

Sin embargo se debe ser consciente del tipo de cambios que se provocarán en el momento de hacer la captura del sistema para preservarlo y entonces poder documentar y justificar cada uno de estos cambios.

3.3. Principio de Locard.

Este principio sugiere que si hubo alguna interacción entre el sistema y el atacante entonces debe haber algún rastro de éste que nos pruebe esta interacción, el reto es encontrar este rastro pues el atacante buscará no dejar ninguno ni quedarse con nada que lo delate.

Este principio fue nombrado por el Dr. Edmon Locard dedicado a la investigación criminal y dice que "Cada contacto deja un rastro" es decir que toda persona o cosa que entre en la escena del crimen dejará un rastro en ella y vice-versa. Así en un escenario de algún crimen podremos encontrar evidencias del criminal y en el criminal encontraremos evidencias que nos confirmen que él estuvo en la escena del crimen.

El objetivo será entonces mostrar una clara relación entre los componentes sospechoso, víctima, la escena del crimen y la evidencia (*Véase fig. 2.4)*.

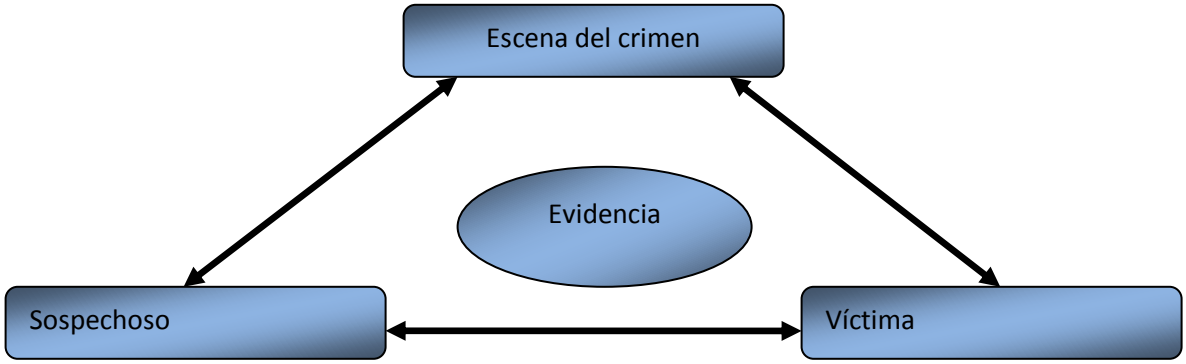


Figura 2.4 Principio de Locard.

Estas son las relaciones que según el principio de Locard se dan en un crimen.

1 El sospechoso se llevará algún rastro de la escena del crimen y de la víctima.

2 La victima tendrá restos del sospechoso y de la escena del crimen.

3 El sospechoso dejará algún rastro en la escena así como la víctima.

A esto se le conoce como el concepto de relación. Es importante recalcar que cualquier cosa podrá ser tomada como evidencia siempre y cuando sirva para establecer o refutar un hecho.

La evidencia puede variar en tamaño y forma, no por ser algo muy pequeño podemos ponerle menos atención. Cada una de las pruebas que se encuentren serán igual de valiosas si ayudan a establecer una relación con el atacante. Es importante cuidar que la evidencia encontrada no se vea alterada o dañada de ninguna manera para que pueda ser válida ante una corte legal.

3.4 Evidencia Digital.

En los puntos anteriores hemos hablado de la evidencia como la parte que se busca dentro de una investigación de cómputo forense, para ser presentada en un procedimiento legal. Por ser la parte fundamental que se busca durante la investigación es imprescindible conceptualizarla.

Dentro de toda la evidencia que se encuentre en la escena del crimen, el cómputo forense se ocupa de la evidencia digital es decir aquella que se pueda encontrar almacenada en algún dispositivo de cómputo.

Existen muchas definiciones para lo que es evidencia digital. A continuación se mencionan algunas que servirán para conceptualizar.

Eoghan Casey define la evidencia digital como "cualquier dato que puede establecer que un crimen se ha ejecutado o puede proporcionar un link entre un crimen y su víctima o un crimen y su autor"[8]

Brian Carrie la definie como "La parte digital que contiene información relevante que apoya o refuta una hipótesis"[9]

El Standard Working Group on Digital Evidence (SVVGDE) la define como "Información de valor probatorio que sea almacenada o transmitida en forma binaria"[10]

De acuerdo con las definiciones anteriores se puede decir que la evidencia digital será todo aquel dato digital que nos proporcione información útil para comprobar o desechar una hipótesis con respecto al incidente. De acuerdo con la

[8] Casey Eoghan. "Digital Evidence and Computer Crime: Forensic Science, Computer, and the Internet". 2004 ISBN 0121631044

[9] Carrier Brian "File System Forensic Analysis". 2005 ISBN 0-32-126817-2

[10] http://www.swgde.org/

evidencia digital obtenida se desarrollan hipótesis que contestan las preguntas acerca de los incidentes. Todo esto se hace bajo métodos científicos.

Cabe mencionar que esta definición será válida solo en el ámbito del análisis forense ya que en el ámbito legal el único que puede determinar a que darle el valor de evidencia es el juez, por lo que al hacer la presentación de la "evidencia digital" obtenida durante la investigación se le tendrá que denominar como hallazgos. Una vez que se estudie el caso y se compruebe que los hallazgos presentados son íntegros -es decir que no ha sufrido modificaciones- y que tiene relevancia en el caso entonces se decidirá si se presenta en el procedimiento legal como evidencia o no.

La evidencia digital no tiene restricciones de tamaño, siempre y cuando sirva para establecer una relación con el atacante. Es así que se puede encontrar evidencia tan pequeña como una dirección IP que tan sólo consta de 4bytes, pero que puede ser suficiente para probar que una red está asociada con el incidente.

Por esta razón al hacer una investigación forense se debe ser muy minucioso y analizar cada uno de los lugares donde sea posible encontrar evidencia. Y una vez que se haya encontrado cuidar que esta se mantenga integra.

Si la integridad de la evidencia se viera violada, ésta ya no podrá presentarse para probar o refutar alguna hipótesis ya que carecerá de confiabilidad por tener la posibilidad de haber sido alterada para el beneficio de alguna de las partes involucradas.

Para conservar la integridad de la evidencia es necesario:

- Evitar se vea alterada.
- Que se tenga una imagen o captura de ésta.
- Que el acceso a ella sea restringido.

- Usar algún método para probar su integridad como puede ser el uso de funciones hash.

Evitar que la evidencia se vea alterada es el punto más importante para poder conservar la integridad de ésta; de este punto dependerán que se puedan realizar los otros tres puntos.

Para asegurar la obtención de la evidencia sin modificaciones se requiere tomar en cuenta su volatilidad, de ello dependerá no sólo que la encontremos sin cambios, sino de que podamos encontrarla aun en el sistema. La volatilidad es la característica que establece el orden en el que se hará la preservación.

3.2.1 Volatilidad.

La volatilidad es el periodo de vida que tienen los datos almacenados en algún dispositivo de cómputo. Este periodo de vida se toma sin considerar que los datos sean eliminados por el usuario.

La volatilidad de los datos es una característica que depende directamente del dispositivo donde se encuentran almacenados los datos.

Dependiendo de esta característica de volatilidad se definen dos tipos de evidencia: la evidencia volátil y la evidencia no volátil. La evidencia volátil es aquella que se encuentra almacenada en dispositivos que para mantener los datos almacenados necesitan estar alimentados de energía eléctrica de manera constante, una vez que está fuente de alimentación se vea interrumpida entonces perderán todo lo que almacenen. Este es el caso de la memoria RAM o la memoria cache.

En cambio la evidencia no volátil es aquella que permanece en el dispositivo aun después de que este pierda la fuente de alimentación eléctrica. Este es el caso de las memorias USB o el disco duro de una computadora.

A continuación se muestra una tabla con el tiempo de vida de los datos volátiles encontrados en una computadora. (*Véase tabla 2.1).*

Tabla 2.1 Clasificación de la información según su periodo de vida.

Registros[11] y memoria cache[12]	Nanosegundos
Memoria (virtual, física)	Nanosegundos
Red local	Milisegundos
Procesos corriendo, archivos abiertos, puntos de montaje en media	Segundos
Sistema de archivos lógicos	Minutos
Discos duros físicos, flopies y respaldos	Años
Cd-Roms	Decenas de años

Para realizar una investigación forense es importante conocer el tiempo de vida que tienen los datos en los diferentes dispositivos ya que esto establecerá el orden de preservación de la evidencia.

Ya que algunos dispositivos sólo mantienen los datos almacenados mientras se encuentran alimentados por algún tipo de energía se puede establecer dos escenarios donde se puede encontrar evidencia digital: Sistemas encendidos o

[11] Es la memoria más rápida de la computadora y la de menor capacidad. Sirve para almacenar los datos con los que está trabajando el CPU y su información de control y estado.

[12] Se utiliza para almacenar una copia parcial del contenido más utilizado por la memoria principal.

vivos –sistemas alimentados por algún tipo de energía- y los sistemas apagados o muertos –son los sistemas que no se encuentran alimentados por ningún tipo de energía- (*Véase fig.2.5)*.

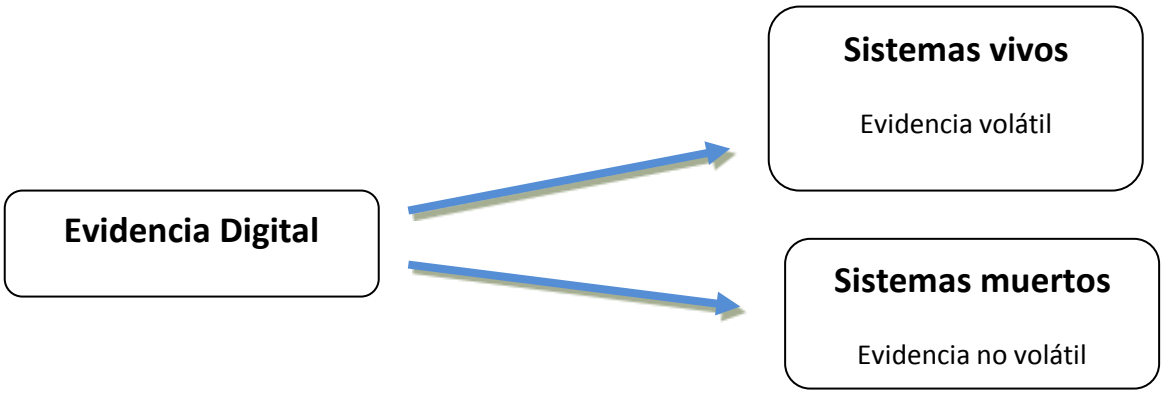


Figura 2.5 Tipos de evidencia digital encontrada en los dos diferentes escenarios.

Como se puede apreciar en la figura 2.5 es en los sistemas vivos donde se puede encontrar la mayor cantidad de evidencia, ya que contamos tanto con la información volátil como con la información no volátil. A continuación se muestra una tabla con los diferentes tipos de datos que se pueden encontrar en un sistema vivo. *(Véase tabla 2.2).*

Tabla 2.2 Características de un sistema vivo.

Características	Datos
Encendido	Datos de memoria
Procesos corriendo	Conexiones de red
Acceso al disco	Procesos
	Discos duros
	Medios removibles
	CD

En los sistemas muertos al no tener alimentación eléctrica se perderán todos los datos que se encontraban almacenados en medios volátiles por ende la cantidad de evidencia que se pueda recuperar será menor. En la tabla que se muestra a continuación se enlistan los tipos de datos que se pueden encontrar en un sistema apagado o muerto *(Véase tabla 2.3)*.

Tabla 2.3 Características de un sistema muerto.

Características	Datos
Desconectado	Discos duros
Sistema apagado	Medios extraíbles
	CD

4. El analista forense y el perito informático.

Para poder cubrir las actividades desarrolladas en el cómputo forense se necesita personal especializado capaz de asegurar el tratamiento correcto del caso, de tal manera que proporcione la ayuda necesaria a la ley. La persona indicada para realizar estas actividades es el analista forense, el cual está capacitado para identificar, preservar, analizar y presentar evidencia digital en un proceso legal.

Todas estas actividades que se realizan al hacer una investigación forense pueden llevarse al cabo sin que el fin sea presentar la investigación ante un juez. Sin embargo si el fin es hacer la investigación dentro de un procedimiento legal se deberán acatar reglas impuestas por la ley y dentro de este ámbito al analista forense se le conocerá como perito informático.

Las reglas federales para el manejo de evidencia de los Estados Unidos de América definen a los peritos informáticos como: “El testigo calificado que por su conocimiento, habilidades, experiencia, entrenamiento o educación puede declarar o dar una opinión sobre una materia técnica, científica o especializada.”

El perito informático es un auxiliar de la justicia que no persigue como objeto resolver un problema operativo sino explicar la causa y la razón de que dichos problemas se hayan presentado luego de haber realizado el análisis y estudio profundo de la evidencia.

El perito informático emitirá sus resultados los cuales deben de estar fuertemente sustentados con bases tanto técnicas como científicas, estas deben de ser objetivas e imparciales.

Una vez que una persona decida participar como perito informático en un procedimiento legal deberá de ser consciente de las implicaciones que esto conlleva.

Una vez que acepta fungir como perito informático posee derechos y obligaciones.

Dentro de los derechos que tiene se encuentras:

- Recibir una contraprestación económica, ya sea que esta se fije por los propios tribunales o por las partes.
- El acceso a los documentos base de la acción.
- Ser notificado en tiempo y forma de plazos de la ley.
- Ser protegido en juicio (juicios orales).
- Ser asistido por un abogado, ya sea el asignado por el juez, o por el contratante.

Dentro de las obligaciones que tiene que cumplir se encuentran:

- Confidencialidad con respecto al asunto en proceso, al contenido de las actuaciones judiciales y al resultado de sus investigaciones.
- Diligencia en el cumplimiento de plazos y formas establecidas por la autoridad.
- Guardar la integridad de la evidencia que encuentre y de los que sean allegados por las partes
- Ser completamente imparcial.
- Construir y mantener la cadena de custodia desde el momento en el que tenga contacto con la evidencia.
- Mostrar un testimonio basado en la suficiencia de hechos y datos.
- El testimonio debe ser producto de principios y métodos confiables.
- El perito deberá aplicar los principios y métodos de manera confiable a los hechos del caso.
- Si dentro de su investigación el perito encontrara pruebas de algún delito como lo es la pornografía infantil se verá obligado a denunciarlo de lo contrario se le podría acusar de complicidad.

Además de cumplir con las responsabilidades antes mencionadas el perito informático deberá ser cuidadoso de acatar todas las reglas establecidas por la ley.

En México para desempeñar la actividad de perito informático dentro de un procedimiento legal se debe cumplir con lo dispuesto en el Código Federal de Procedimientos Penales de México el cual establece los requerimientos y obligaciones de los peritos informáticos en los artículos 223, 224, 225, 227, 228, 234 y 235. *(Véase tablas 2.4 y 2.5)*

Tabla 2.4 Requerimientos para desempeñar la actividad de perito en informática establecidos en el Código Federal de Procedimientos Penales de México.

Artículo 223	Que los peritos deberán tener título oficial en la ciencia o arte que se refiere el punto sobre el cual deba dictaminarse, si la profesión o arte están legalmente reglamentadas; en caso contrario se nombraran peritos prácticos.
Artículo 224	También podrán ser nombrados peritos prácticos cuando no hubiere titulados en el lugar en que se siga la instrucción; pero en este caso se librará exhorto o requisitoria al tribunal del lugar en que los haya, para que en vista del dictamen de los prácticos emitan su opinión.
Artículo 225	Se establece que la designación de peritos hecha por el tribunal o por el Ministerio Publico deberá recaer en las personas que desempeñen ese empleo por nombramiento oficial y a sueldo fijo, o bien en personas que presten sus servicios en dependencias del Gobierno Federal, en Universidades del país, o que pertenezca a Asociaciones de Profesionistas reconocidas en la república.

Tabla 2.5 Obligaciones de los peritos informáticos establecidas en el Código Federal de Procedimientos Penales de México.

Artículo 227	Los peritos que acepten el cargo, con excepción de los oficiales titulares, tiene obligación de protestar su fiel desempeño ante el funcionario que practique las diligencias.
Artículo 228	El funcionario que practique las diligencias fijará a los peritos el tiempo en que deban cumplir su cometido. Si transcurrido ese tiempo no rinden su dictamen o sí legalmente citados y aceptado el cargo, no concurren a desempeñarlo, se hará uso de alguno de los medios de apremio. Si a pesar de haber sido apremiado el perito no cumple con las obligaciones impuestas en el párrafo anterior, se hará su consignación al Ministerio Público para que proceda por el delito a que se refiere el artículo 178 del Código Penal.
Artículo 234	Los peritos practicarán todas las operaciones y experimentos que su ciencia o arte les sugiera y expresarán los hechos y circunstancias que sirvan de fundamento a su opinión.
Artículo 235	Los peritos emitirán su dictamen por escrito y lo ratificarán en diligencia especial. Los peritos oficiales no necesitarán ratificar sus dictámenes, sino cuando el funcionario que practique las diligencias lo estime necesario. En esta diligencia el juez y las partes podrán formular preguntas a los peritos.

Cuando un analista forense se desempeña como perito informático es recomendable que se encuentre asesorado por un abogado ya que no solo requerirá tener conocimiento en informática sino también en leyes que le aseguren llevar un caso con éxito y no incurrir en faltas.

Dentro de las actividades que debe realizara el perito informático se encuentran:

- Identificación y recolección de evidencia.
- Aplicación de procedimientos de revisión y análisis forense.
- Comprensión y práctica de los estándares de ética que rigen las ciencias forenses de la informática.
- Aplicación de conocimiento de los aspectos legales sobre la privacidad y adquisición y revisión de medios magnéticos.
- Mantenimiento de la cadena de custodia durante todo el procesos de una investigación forense
- Aplicación de conocimientos en los diferentes tipos sistemas de archivos asociados a los diferentes tipos de sistemas operativos, acceso a archivos temporales, de cache, correo electrónico, de Web etc.
- Conducir de manera detallada la recuperación de datos de todas las particiones del o de los discos
- Aplicación de técnicas para romper contraseñas de seguridad
- Redacción del peritaje hecho a las pruebas de una manera clara para todo público evitando el lenguaje técnico.
- Asistir a dar su testimonio frente al juez.

Todas estas actividades se llevaran a cabo en distintos momentos de la investigación forense. Una investigación forense cuenta al menos con cuatro fases o etapas, en las que se engloban las diferentes actividades antes mencionadas.

5. Etapas generales de una Investigación Forense.

Para poder realizar una investigación forense se han definido cuatro etapas en donde se engloban las actividades que se debe de desarrollar el analista forense *(Véase fig. 2.6).* Estas cuatro etapas son:

- Identificación.
- Preservación del sistema.
- Análisis.
- Presentación.

Estas etapas no necesariamente deben desarrollarse de manera consecutiva, es probable que desarrollando la etapa del análisis se encuentre nueva evidencia y se tenga que desarrollar por segunda vez la etapa de preservación. Aunque en el caso ideal se busca la obtención total de la evidencia necesaria para poder hacer la reconstrucción de los hechos desde la primera vez y no correr el riesgo de que la evidencia se vea modificada o eliminada.

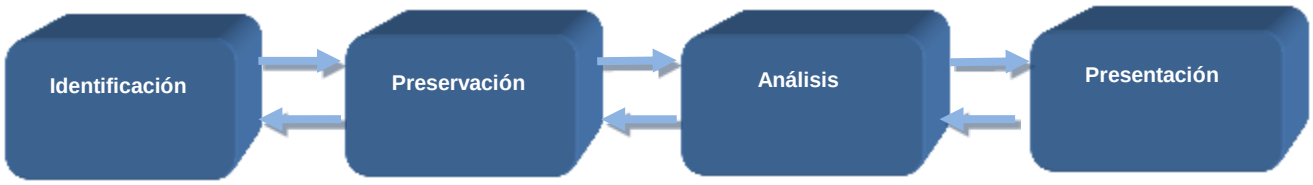


Figura 2.6 Etapas generales de una investigación de cómputo forense.

A continuación se describirán cada una de las etapas mencionando cuales son los objetivos, las actividades realizadas, las herramientas que se pueden utilizar, las reglas que marca la ley para poder presentar el caso en un procedimiento legal y si existe algún manual de buenas prácticas.

5.1. Identificación.

Esta será la etapa inicial de la investigación forense, tiene como objetivos:

- Reconocer dentro de la escena del crimen los dispositivos que contienen los datos necesarios para poder hacer la reconstrucción de los hechos.
- Determinar las características de los dispositivos contenedores de evidencia, esto servirán para poder realizar la siguiente etapa que es la de preservación.

Para poder cumplir con estos objetivos las actividades que se realizan son:

- Creación de cuestionarios dirigidos al personal que de alguna manera está relacionado con el sistema afectado, con la finalidad de determinar el crimen y poder intuir donde se encuentra la evidencia.

Estos cuestionarios pueden ser escritos o hablados.

Una vez determinados los dispositivos contenedores de evidencia entonces se hará una descripción específica de ellos, en donde se debe de incluir

- Tipo de hardware del equipo
- En qué manera se encuentra (apagado o prendido)
- Tipo de sistema operativo que contiene
- Accesorios o periféricos conectados al equipo
- Si posee conexión a internet
- Si posee firewall
- Si está en el ámbito del DMZ (Zona desmilitarizada)
- Cuantos equipos hay en la red etc.

Para la realización de la identificación del dispositivo y su estado se debe ser lo más descriptivo que se pueda, evitando pasar algún detalle por alto que pudiera causar la duda de la validez de la evidencia. Es por ello que se debe de tomar nota de todo lo que se encuentra, así como fotos y/o video.

Con todos estos datos se levanta la cadena de custodia la cual tiene como fin mantener la integridad de la evidencia, para que esta sea válida en el proceso legal. Para esto se tienen que llenar dos tipos de formatos.

- Bitácora de custodia de la evidencia
- Bitácora de acceso a la evidencia

En la bitácora de custodia de la evidencia se hace la descripción del dispositivo, la descripción de su estado y quien fue el responsable de su identificación.

El formato de esta bitácora puede ser creado según las necesidades del analista forense, sin olvidar que este tiene como objetivo guardar la integridad de la evidencia. Por lo cual debe de contestar las siguientes preguntas:

- ¿Quién capturo la evidencia?
- ¿Cómo y dónde fue encontrado el dispositivo contenedor de la evidencia?
- ¿Quién tomo posesión de la evidencia?
- ¿Cómo era el dispositivo contenedor de evidencia y como fue protegido durante la captura?
- ¿Quién tomo las pruebas para almacenamiento y por qué?

Algunas veces la realización de una investigación de cómputo forense no la hace una sola persona, en estos casos es cuando se hace indispensable usar las bitácoras de acceso a la evidencia, en donde se registran los nombres de las

personas que tienen acceso a la evidencia especificando la fecha y la hora en la que entran en contacto con la evidencia, así como el registro del momento en el que la dejan y el nuevo responsable.

Con esto se logra tener el control completo de todas las personas que tienen contacto con la evidencia. Se sugiere que el acceso a ella sea restringido.

A continuación se muestran algunos ejemplos de bitácoras de custodia y bitácoras de acceso a la evidencia *(Véase fig. 2.7)*.

<table>
<tr><td colspan="4">El artículo(s) que se describe a continuación se obtuvieron como prueba por el suscrito durante una investigación oficial de la: (nombre de la escuela, distrito o entidad)</td></tr>
<tr><td colspan="4">Descripción del articulo</td></tr>
<tr><td colspan="4">Obtenido desde: (titulo, nombre, localización, número de teléfono)</td></tr>
<tr><td>Nombre del investigador:</td><td colspan="2">Firma del Investigador:</td><td>Fecha de Obtención:</td></tr>
<tr><td colspan="4">Numero de caso:</td></tr>
<tr><td colspan="4">Disposición transitoria de este (os) articulo (s): Donde se almacena (n)</td></tr>
<tr><td>Liberado por: (nombre y firma)</td><td colspan="2">Liberado para: (nombre y firma)</td><td>Fecha:</td></tr>
<tr><td colspan="4">Disposición transitoria de este (os) articulo (s): Donde se almacena (n)</td></tr>
<tr><td>Liberado por: (nombre y firma)</td><td colspan="2">Liberado para: (nombre y firma)</td><td>Fecha:</td></tr>
<tr><td colspan="4">Disposición transitoria de este (os) articulo (s): Donde se almacena (n)</td></tr>
</table>

Figura 2.7 Formato de cadena de custodia.

El formato de cadena de custodia puede ser tan específico como uno lo desee. Los formatos que se muestran a continuación son mucho más detallados que el anterior. El primero de estos formatos muestra el registro de evidencia de una computadora, y el segundo está dirigido al registro de discos duros de computadoras *(Véase fig. 2.8 y 2.9)*.

Case Number: _____ **Exhibit Number:** _____

Laboratory Number: _____ **Control Number:** _____

Computer Information

Manufacturer: _____ Model: _____

Serial Number: _____

Examiner Markings: _____

Computer Type: Desktop ☐ Laptop ☐ Other: _____

Computer Condition: Good ☐ Damaged ☐ **(See Remarks)**

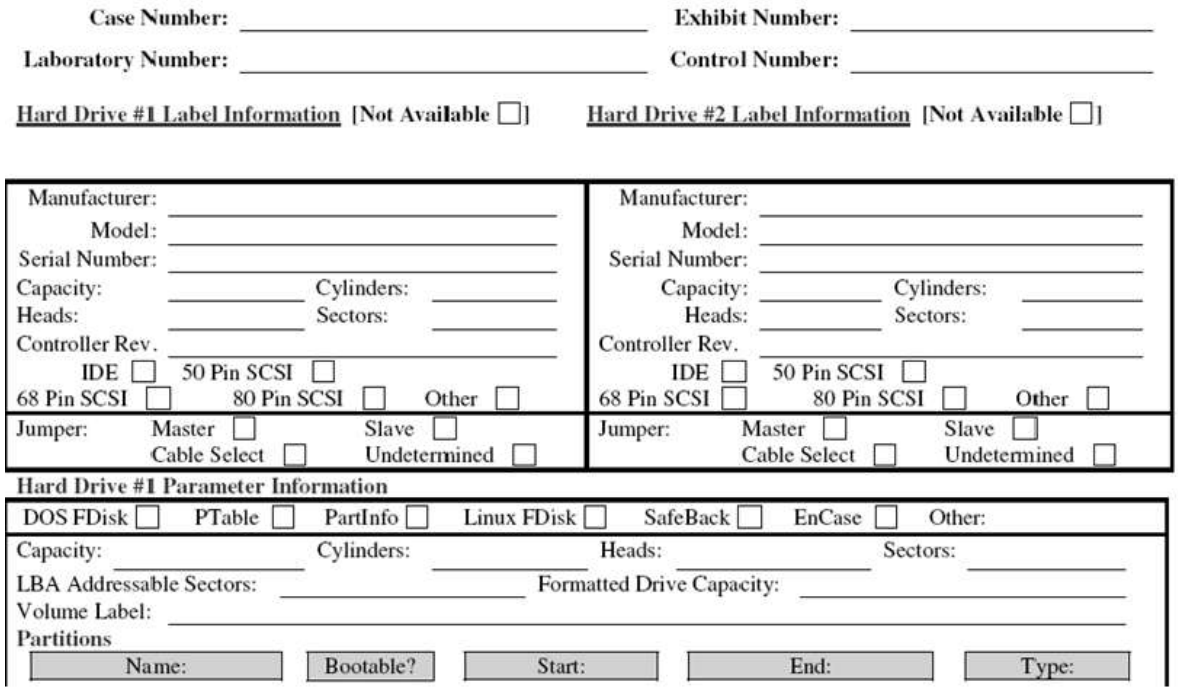
Number of Hard Drives: _____ 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☐ Tape Drive ☐ Tape Drive Type: _____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☐ Other: _____

Figura 2.8 Formato de custodia para una computadora.



Case Number: _____ Exhibit Number: _____

Laboratory Number: _____ Control Number: _____

Hard Drive #1 Label Information [Not Available ☐] Hard Drive #2 Label Information [Not Available ☐]

Hard Drive #1 Label Information	Hard Drive #2 Label Information
Manufacturer:	Manufacturer:
Model:	Model:
Serial Number:	Serial Number:
Capacity: Cylinders:	Capacity: Cylinders:
Heads: Sectors:	Heads: Sectors:
Controller Rev.	Controller Rev.
IDE ☐ 50 Pin SCSI ☐	IDE ☐ 50 Pin SCSI ☐
68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐	68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐
Jumper: Master ☐ Slave ☐	Jumper: Master ☐ Slave ☐
Cable Select ☐ Undetermined ☐	Cable Select ☐ Undetermined ☐

Hard Drive #1 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:

Figura 2.9 Formato de custodia para un disco duro.

5.2. Preservación del sistema.

Esta etapa tiene como objetivo:

- Hacer la recolección de la evidencia.
- Reducir la pérdida de la evidencia.
- Mantener la integridad de la evidencia.

Para poder cumplir con este objetivo se tendrán que realizar actividades como:

- Establecer el orden de preservación (dependiendo de la volatilidad).
- La captura de la evidencia.
- La duplicación de la evidencia.

- La implementación de mecanismos que ayuden a la verificación de la integridad de la evidencia.
- Resguardo de la evidencia.

A.Establecer el orden de preservación.

En la etapa anterior –identificación- se hizo la identificación de los dispositivos que pudieran contener evidencia. En esta etapa es necesario establecer el orden en el que se hará la preservación de la evidencia para evitar que esta cambie o desaparezca. Esto se lograra tomando en cuenta el orden de volatilidad de los datos.

B.La captura de la evidencia.

Dependiendo de donde se encuentre la evidencia será el procedimiento de preservación y la elección de herramientas necesarias para lograrlo. Una de las técnicas más utilizadas para realizar la preservación de evidencia es la realización de imágenes forenses.

Las imágenes forense son copias bit a bit de un dispositivo que garantiza obtener todos los datos existentes en el medio tal como si este hubiese sido clonado. Al analizar la imagen forense se podrá encontrar la información almacenada en cada uno de los sectores del disco sin importar el estado que tengan los sectores –asignado o no asignado-. Esta es una de las ventajas que obtenemos en comparación con una copia común en donde no podríamos ver el contenido de los sectores no asignados. Al hacer una copia bit a bit no perdemos información de la capa de metadatos ni la modificamos.

Las imágenes forenses se pueden realizar en cualquiera de los dos escenarios –sistemas vivos o prendidos y sistemas muertos o apagados- A continuación se muestra una tabla con los consejos que da “la guía de buenas

prácticas para la captura y almacenamiento de evidencia" [RFC 3227] para conservar la integridad de la evidencia durante la captura *(Véase tabla 2.8).*

Tabla 2.6 Consejos para conservar la integridad de la evidencia dados en el RFC 3227.

Conservación de la integridad
Si el sistema se encuentra vivo no sea apagado hasta que se haya completado la captura de evidencia.
No se confíe en los programas que se encuentren en el sistema.
No se corran programas que puedan modificar la fecha y hora de acceso de los archivos.

Al realizar una imagen forense es importante tener en cuenta las reglas de privacidad que han sido establecidas en el lugar donde se encuentre el dispositivo que almacena la evidencia, así como la jurisdicción legal que rija en ese lugar. Es importante no irrumpir en ninguna regla al menos que se tenga una fuerte justificación.

Las imágenes forenses se pueden hacer de tres formas diferentes.

- Bit a bit de disco a disco.
- Bit a bit de disco a archivo.
- Copias aisladas de archivo(s) y/o carpeta(s).

Para la copia bit a bit de disco a disco. La copia depende de la geometría del disco y las herramientas que podemos encontrar para hacer este tipo de imágenes son:

- Norton Ghost
- SafeBack
- SnapCopy

Todas estas permiten el ajuste de la geometría.

La copia bit a bit de disco a archivo es el método más flexible, permite múltiples copias y es la forma en que generalmente trabajan las herramientas de duplicación, algunos ejemplos de estas son:

- EnCase
- FTK
- Dd
- Dcfldd

El último tipo que son las copias aisladas de archivo(s) y/o carpeta(s) es conveniente cuando encontramos discos muy grandes o arreglos de discos (RAID) o para cuando no se dispone del tiempo para realizar la copia total del disco o bien cuando la investigación se centra en algún tipo de aplicación como puede ser el correo electrónico (archivos PST).

Algunas de las herramientas que podemos encontrar son:

- EnCase
- Forensic Tool Kit
- Dd
- Dcfldd

La imagen forense obtenida puede ser almacenada en tres diferentes formatos:

- Raw
- Propietario
- Advanced Forensics Format (AFF[13])

El formato *Raw* hace posible escribir la imagen en un archivo, tiene la ventaja de que la transferencia de datos es rápida, puede ignorar errores menores de adquisición de datos de un drive, y la mayoría de las computadoras pueden leer archivos con este tipo de formato. La extensión que usa es .dd.

La desventaja de utilizar este formato es que se necesita tener un disco con la misma capacidad de almacenamiento que la que tiene el disco al que se le desea hacer la imagen forense.

El formato de datos *propietarios.* Este formato tiene la opción de compresión en las imágenes adquiridas, también puede dividir las imágenes en archivos segmentados y puede integrar metadatos en el archivo que contiene la imagen.

Algunas de las desventajas son: no es posible usar este tipo de imágenes con diferentes herramientas, el tamaño del archivo segmentado está limitado.

Forense de formato avanzado. Este formato proporciona la opción de obtener imágenes comprimidas, no tiene restricción de tamaño para la generación de imágenes, proporciona espacio en el archivo de la imagen o archivos segmentados para los metadatos. También nos permite la verificación de consistencia interna para auto-autenticación.

[13]El formato AFF es de código abierto.

Las extensiones que maneja son:

- .afd para archivos de imágenes segmentados
- .afm para metadatos AFF

Para la realización de la imagen forense utilizando cualquiera de los métodos y formatos que anteriormente describimos es recomendable que se utilicen medios completamente limpios[14] y que se puedan proteger contra escritura

Para poder realizar la imagen forense de un dispositivo se necesita contar con los respectivos cables para su alimentación. Es necesario contar con un vasto conjunto de equipo físico, ya que la evidencia puede encontrarse en computadoras, celulares, impresoras, switch, Xbos, ipods, tabletas electrónicas etc.

Existen maletines forenses equipados con los cables esenciales para poder realizar la preservación de la evidencia *(Véase fig. 2.10).*

Figura 2.10 Maletín Forense.

[14] Se entiende que un dispositivo está limpio cuando este no contienen información previa.

Todo el procedimiento llevado a cabo para la captura de la evidencia debe ser detallado en un documento, donde se justifique cada una de las acciones llevadas a cabo, el método utilizado debe de ser transparente y reproducible.

C.Duplicación de la evidencia.

Una vez terminada la captura de evidencia se debe realizar la duplicación de esta imagen obtenida, esto es recomendable para evitar la pérdida parcial o total de la evidencia durante el proceso.

Con el fin de conservar la integridad de la evidencia habrá que realizar una o varias copias según las necesidades, uno de estos duplicados deberá de resguardarse intacto y los otros estarán disponibles para ser utilizados durante las diferentes pruebas y por los diferentes usuarios.

Todas estas copias deberán de ser verificadas por algoritmos matemáticos que comprueben que se trata de una duplicación exacta y por lo tanto fiable. Este mecanismo que garantiza la integridad de la evidencia se debe conservar durante todo el proceso de la investigación para probar que a pesar de las pruebas realizadas en la evidencia esta no se vio alterada de ninguna manera.

El acceso a los duplicados de la imagen debe ser restringido y controlado.

D. Implementación de mecanismos que ayuden a la verificación de la evidencia.

Existen diferentes técnicas que ayudan a la conservación de la integridad de la evidencia. A continuación se muestra un listado con algunas de estas técnicas. Generalmente se utilizan más de una técnica para guardar la integridad de la evidencia.

- El uso de funciones hash.[15]
- Uso de sellos y cintas de evidencia.
- Protección contra escritura en los dispositivos.
- Uso de bolsas de faraday.
- Cuidado del medio ambiente.

a) Uso de funciones hash.

Éstas son implementadas en varias herramientas que nos ayudan a capturar la imagen forense. Este valor hash puede ser recalculado cada vez que se desee para comprobar que la evidencia no ha sido modificada.

Es importante mencionar que el hash debe de ser externo de la imagen es decir no deberá de formar parte de la imagen, si el hash formara parte de la imagen se correría el riesgo de que al ser modificada la evidencia el hash se recalculara y se guardara como el legitimo y de esta manera no estaría proporcionando ningún tipo de integridad.

b) El uso de sellos y cintas de evidencia.

Esta técnica se usa sobre todo para la evidencia que se requiere transportar hasta los laboratorios donde se le dará el tratamiento necesario. En este caso debemos de asegurarnos que ninguna persona no autorizada tenga acceso a ella durante el traslado.

Para tal motivo se guarda el dispositivo bien etiquetado -es decir que la etiqueta lo defina y lo identifique- en cajas o bolsas que a su vez serán selladas con “sellos de seguridad”, este tipo de sellos son aquellos que su duplicación es difícil y la alteración de estos es evidente, para lograr un

[15] Véase el capítulo 1, subtema criptografía.

sello como estos lo más común es firmar la cinta con la que son sellados para que esta no pueda ser remplazada.

c) La protección contra escritura en los dispositivos.

La protección contra escritura en los dispositivos es una medida que es importante implementar para que la evidencia se conserve integra aún después de del análisis forense. Se protege a la evidencia de posibles alteraciones provocadas deliberadamente o por descuido.

Este tipo de protección se puede hacer por medio de hardware o software. Por medio de hardware al usar dispositivos que no permitan la sobre-escritura como es el caso de los CD-R o los discos duros que cuentan con el seguro que permite conectarlo para tener acceso de sólo lectura.

Por medio de software existen programas que permiten establecer ciertos dispositivos como de sólo lectura aunque estos permitan la sobre-escritura.

d) Uso de bolsas de faraday.

Este tipo de bolsas protegen los dispositivos electrónicos de algún daño causado por campos magnéticos, en el caso de los celulares además de protegerlos de campos magnéticos los aíslan de la red telefónica garantizando que la información no se verá modificada por información entrante.

La importancia de proteger los equipos de campos magnéticos es porque se evita la alteración o la eliminación de la información que se encuentra almacenada en el dispositivo. De hecho el usar campos magnéticos es una práctica utilizada para garantizar la eliminación de información de algún

almacenamiento electromagnético –magnetización o Degaussing[16]- *(Véase subcapítulo 4.1 sistema de archivos. Capítulo Primero)*.

e) Cuidado del medio ambiente.

Por último hay que tener en cuenta los factores ambientales que puedan dañar la evidencia contenida en los dispositivos computacionales. Algunos de los factores ambientales que pueden dañar los dispositivos son: la temperatura y la humedad.

E. Resguardo de evidencia.

La evidencia debe de ser almacenada en un lugar seguro, al cual se tenga el acceso restringido, además de que cualquier acceso debe de estar claramente documentado y registrado en la cadena de custodia, todo esto con el fin de detectar cualquier acceso no autorizado.

Además de tomar en cuenta todos los puntos anteriormente descritos se tiene que cumplir con ciertas normas impuestas tanto por la entidad a la que se le está haciendo la investigación forense como a las normas impuestas por el estado. En este caso se verán las normas establecidas en el código federal de procedimientos penales de México, en los artículos 123 Bis, 181, 269 y 289Bis en los cuales se estipulan las actividades con las que se debe cumplir para realizar la preservación de evidencia *(Véase tabla 2.7)*.

[16] Es la actividad por la cual se eliminan los campos magnético del dispositivo, es una de las técnicas recomendadas por la NSA

Tabla 2.7 Requerimientos para preservar evidencia establecidos en el Código Federal de Procedimientos Penales de México.

Artículo 123 Bis	La preservación de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito es responsabilidad directa de los servidores públicos que entren en contacto con ellos. En la averiguación previa deberá constar un registro que contenga la identificación de las personas que intervengan en la cadena de custodia y de quienes estén autorizadas para reconocer y manejar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito. Los lineamientos para la preservación de indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito, que por acuerdo general emita la Procuraduría General de la República, detallarán los datos e información necesaria para asegurar la integridad de los mismos. La cadena de custodia iniciará donde se descubra, encuentre o levante la evidencia física y finalizará por orden de autoridad competente.
Artículo 181	Los instrumentos, objetos o productos del delito, así como los bienes en que existan huellas o pudieran tener relación con éste, serán asegurados a fin de que no se alteren, destruyan o desaparezcan. El Ministerio Público, las policías y los peritos, durante la investigación y en cualquier etapa del proceso penal, deberán seguir las reglas referidas en los artículos 123 Bis a 123 Quintus. La administración de los bienes asegurados se realizará de conformidad con la ley de la materia.
Artículo 269 Bis	El tribunal recibirá las pruebas documentales que le presenten las partes hasta un día antes de la citación de la audiencia de vista, y las agregará al expediente, asentando razón en autos.
Artículo 289	Cuando durante el procedimiento a que se refieren los artículos 123 Bis a 123 Quintus de este Código, los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito, se alteren, no perderán su valor probatorio, a menos que la autoridad competente verifique que han sido modificados de tal forma que hayan perdido su eficacia para acreditar el hecho o circunstancia de que se trate. Los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito, en los casos a que se refiere el párrafo anterior, deberán concatenarse con otros medios probatorios para tal fin.

5.3. Análisis.

Esta etapa tiene como objetivos:

- Examinación y evaluación de la información.
- Interpretación de los datos recuperados.
- Creación de un escenario de los hechos ocurridos con base en los datos encontrados.
- Mantener la evidencia integra.

Para lograr los objetivos mencionados se realizan actividades como:

- Preparación.
- Extracción de datos.
- Interpretación de los datos.

a) Preparación.

Dentro del proceso de preparación se hará la configuración del equipo necesario para hacer el análisis (estación forense), se ubicara tanto el equipo como la evidencia en un lugar seguro y con las condiciones necesarias para no dañar la evidencia (laboratorio forense) y se dividirán los datos que se hayan recolectado según sus características para facilitar el tratamiento que se les tenga que dar.

A continuación se muestra una división de los datos dependiendo de la fuente de donde fueron extraídos *(Véase fig. 2.11)*. Generalmente los datos que son extraídos de una misma fuente requieren ser analizados con las mismas técnicas y las mismas herramientas por lo cual dividirlos de esta forma puede ahorrar tiempo en el momento de hacer el análisis

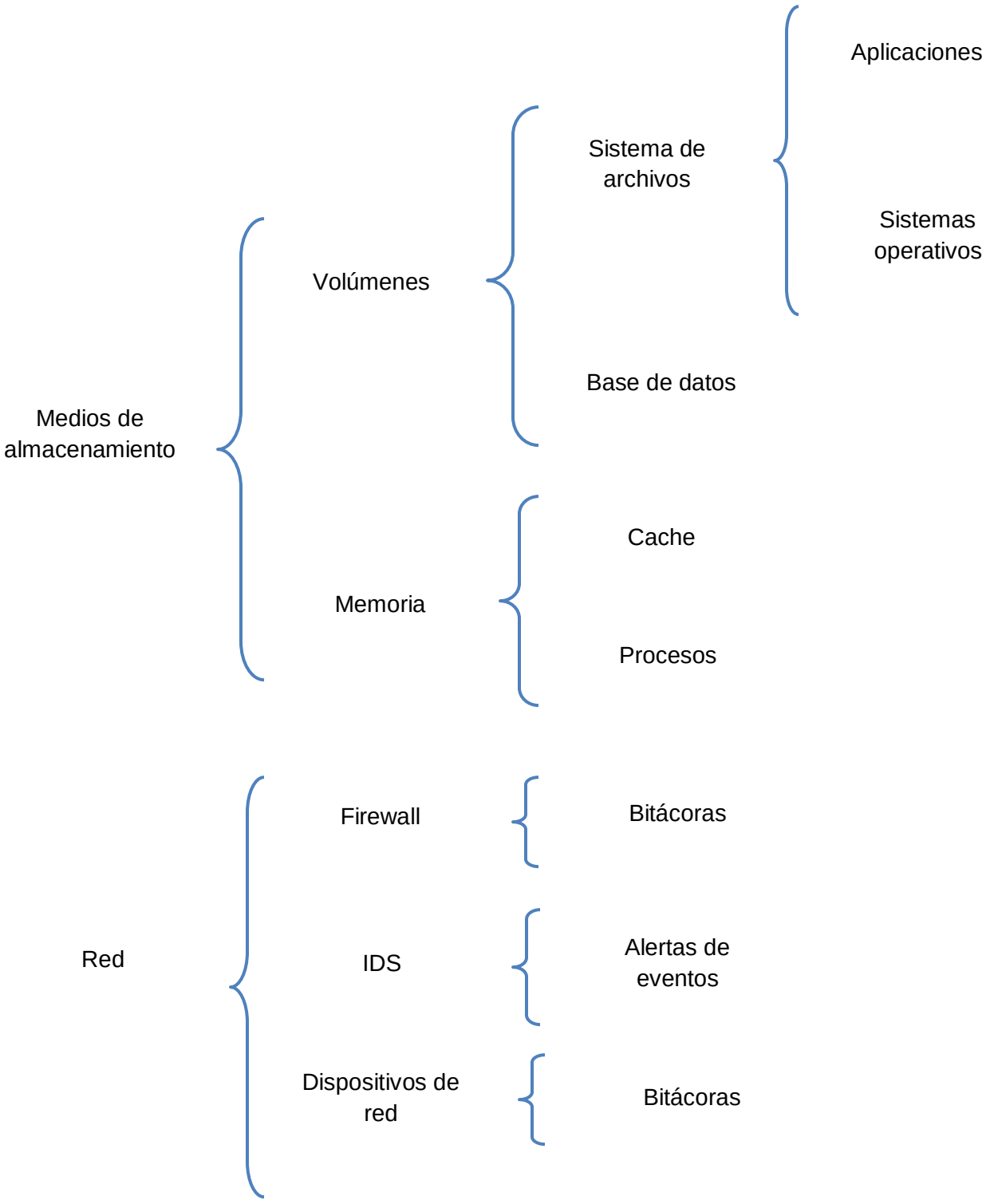


Figura 2.11 División de datos según su fuente de extracción.

Una vez que se hace la división de la evidencia según su fuente de extracción se procederá a realizar su análisis con las herramientas y técnicas pertinentes, para esto se deberá de contar con equipo especializado y configurado correctamente para dicha actividad. A este equipo se le conocerá como estación forense.

La estación forense posee una configuración especial tomando en cuenta sobre todo que en ella se conectara la evidencia y ésta no puede ser alterada por ninguna razón, se suele configurar para que todo aquel dispositivo que desee conectarse a la estación forense tenga que hacerlo en modo de sólo lectura o bien a través de bloqueadores de escritura.

Tomando en cuenta que la evidencia se pude encontrar almacenada en cualquier tipo de dispositivo se requiere que la estación forense este equipada con los diferentes conectores que existen en el mercado y los cables de alimentación necesarios.

Finalmente la estación forense debe de contar con varios sistemas operativos y herramientas para el análisis de los diferentes tipos de datos, es útil contar con software dedicado a la adquisición, análisis y creación del reporte, es importante que estas herramientas soporten los diferentes formatos y además sean confiables[17].

Adicionalmente debemos contar con editores de texto y programas de visualización de gráficos.

Esta estación forense deberá de estar ubicada en un lugar seguro y con las condiciones ambientales necesarias para hacer el análisis de la evidencia extraída. A este lugar se le conoce como laboratorio forense.

[17]Una herramienta es confiable cuando provienen de una fuente segura es decir que el proveedor nos garantiza que no está contaminada con código malicioso.

Dentro del laboratorio forense se deberá de contar con un espacio de almacenamiento físico seguro en el cual se pueda resguardar la evidencia y restringir el acceso a ella.

b) Extracción de datos.

Durante la extracción de datos se buscará hacer la recuperación de los datos almacenados sin considerar los archivos que se encuentran en el sistema de archivos. Principalmente se buscará obtener datos que se encuentren el *slack space* o los archivos que fueron borrados y se encuentren es clusters no asignados.

También se busca obtener información como: su nombre, tamaño, localización, fecha de creación, fecha de modificación, directorio donde se almacena y usuario propietario. Se busca la obtención de éste tipo de información tanto de los archivos disponibles en el sistema de archivos como de los que no lo están.

De tener razones suficientes para analizar archivos protegidos se tendrá que realizar la obtención de contraseñas y recuperar archivos cifrados.

c) Interpretación de los datos.

Para poder interpretar los datos extraídos se tendrá que determinar si estos forman parte significativa para poder resolver el caso, posteriormente se recomienda establecer una línea de tiempo donde se registre cada uno de los hechos encontrados para así poder hacer una representación de lo sucedido. De forma paralela formularan hipótesis con los datos encontrados.

Para crear la línea del tiempo es importante conocer los tiempos MAC[18] de los archivos. Es decir las fechas y horas de creación modificación y acceso de cada uno de los archivos relevantes para el caso e identificar que usuario utilizó estos archivos, así como quién o quiénes lo poseen. Analizar los metadatos.

Algunos datos más que pueden ubicarse en la línea del tiempo y ayudarían a reconstruir los hechos ocurridos son: las bitácoras del sistema, las bitácoras de servidores, archivos temporales, archivos ocultos, archivos borrados, mensajes de correo, las alertas de eventos de algunos programas y el uso de las aplicaciones.

Las hipótesis formuladas durante el proceso de investigación ayudarán al analista a formar escenarios de los posibles hechos y con ello el analista identificará cuáles son los posibles lugares en donde se halla la evidencia. Esta técnica ayuda a reducir el tiempo de análisis, va discriminando datos y se centra sólo en los lugares involucrados.

Al hacer las hipótesis hay que tener muy claro que tendrán que irse ajustando según los datos encontrados y no al revés. Sería un grave error intentar ajustar los datos en las hipótesis realizadas pues se perdería el objetivo y es probable que se llegue a un resultado equivocado.

Es importante que todas las actividades que se realicen en el análisis sean documentadas por dos principales razones: la primera para que se pueda demostrar que se ha mantenido la cadena de custodia en todo momento y comprobar que todas las actividades realizadas tienen una justificación y la segunda para que el resultado pueda ser reproducible en cualquier momento y comprobar que es fiable.

[18]MAC por sus siglas en Ingles (Modify Access Change) significa Modificación Acceso Cambio y son registros de la última modificación acceso y/o cambio de los archivos.

5.4. Presentación.

Esta etapa tiene como objetivo la creación del reporte que se entregará como resultado final de la investigación forense.

Este reporte estará conformado por:

- Descripción o Resumen del caso.
- Documentación de la adquisición y preparación para la evidencia.
- La descripción de cada una de las acciones realizadas durante el análisis.
- Una conclusión.
- Anexos.

La descripción o resumen del caso: Esta sección tendrá una longitud variable. Incluirá toda la información que explique cómo fue que el analista forense se involucró con la evidencia y desde que momento tuvo contacto con ella. Puede ser que el analista forense tuviera contacto con la evidencia sólo después de que esta fue preservada. Por lo que es necesario especificar esos detalles y cómo fue que se mantuvo la cadena de custodia.

Documentación de la adquisición y preparación de la evidencia: En esta sección se describirá en detalle cómo fue encontrada la evidencia y cuáles fueron las medidas que se tomaron para conservar y adquirir la evidencia forense. Es muy importante detallar la interacción con la evidencia digital

En esta sección del documento se incluirán fotos, formatos de cadena de custodia, capturas de pantalla y toda aquella prueba que se tenga para demostrar que se ha conservado la integridad de la evidencia.

También se describirá el método que se utilizó para realizar la imagen forense de la evidencia.

Para realizar *la descripción de cada una de las acciones realizadas durante el análisis* es importante que se mencione puntualmente cada una de las actividades que se llevo a cabo durante el análisis, así como las herramientas que se utilizaron.

Esta es la sección que tiene que estar más detallada ya que si alguna persona desea comprobar los resultados debe de contar con toda la información para poder reproducir las pruebas que se describen.

Es aconsejable que se adjunten capturas de pantalla donde se muestre las actividades que se están describiendo. Para facilitar la navegación del lector por el documento se sugiere que se le incluyan hipervínculos al informen que lo lleven a las fotos, documentos o cualquier otra cosa que se desee mostrar.

La *conclusión* se redactará con base en la evidencia forense encontrada y analizada. Recordando que el objetivo es denunciar los hechos sin importar si estos son inculpatorios o exculpatorios.

En algunos casos donde la investigación forense se desarrolla dentro de un procedimiento legal se pide que se conteste puntualmente a algunos cuestionamientos que servirán para deliberar el caso. Es responsabilidad del analista forense contestar a cada uno de ellos.

Se aconseja que la realización del reporte no se deje como una tarea final, que se realice a la par del desarrollo de la investigación pues de esta forma es más probable que no se olvide anexar ningún detalle.

Para poder desarrollar un buen reporte es necesario contar con todos los detalles encontrados durante la investigación, es importante tomar notas durante todo el procedimiento. Las notas pueden ser escritas o bien el analista forense se puede apoyar en grabaciones, fotografías o videos.

En los *anexos* se puede adjuntar información que sirva de apoyo a la evidencia encontrada: fotografías, videos, planos de las construcciones, contratos, reglamentos, etc.

El reporte es un documento confidencial mientras este se encuentra en proceso de elaboración, una vez entregado al juicio, empieza a ser público.

6. Delitos informáticos.

Las tecnologías de información han evolucionado tan rápido cambiando la vida social que ha sido imposible que el derecho evolucione a la par regulando cada conducta ilícita que surja. Primero porque para que se pueda regular una actividad de este tipo esta tiene que manifestarse, las leyes no pueden anticiparse y regular algo que no existe.

Por otro lado es necesario que personas con formación de abogados comprendan tópicos técnicos y tecnológicos para que de esta forma puedan legislarlos.

En México la legislación de delitos informáticos se ha quedado muy rezagada con respecto a las exigencias. Sin embargo existe regulación en la materia que es importante conocer.

6.1 Legislación informática en México.

En México existe legislación informática para los delitos informáticos, la propiedad intelectual, los contratos electrónicos y firma digital, bases de datos y cómputo forense.

A continuación se muestra una tabla de los campos donde existe legislación informática en México y en que código o ley se encuentran regulados *(Véase tabla 2.8).*

Tabla 2.8 Legislación Informática en México.

Legislación Informática en México.	
Delitos Informáticos	○ Código Penal Federal. ○ Ley federal del Derecho de Autor. ○ Ley Federal de Protección de datos personales. ○ Regulaciones a nivel federal
Propiedad intelectual	○ Ley Federal del Derecho de Autor ○ Ley de Propiedad Industrial
Correo Electrónico	○ Código Penal Federal
Contratos electrónicos (firma digital)	○ Código de comercio ○ Código Civil Federal ○ Ley de Mercado de Valores
Bases de Datos	○ Ley Federal de Protección de Datos Personales
Cómputo Forense	○ Código de comercio. ○ Código Federal de Procedimientos Civiles. ○ Código Penal Federal.

La legislación que existe para el correo electrónico se centra en la privacidad y el spam y dentro de la legislación de que existe para el cómputo forense esta es referida a la evidencia electrónica.

6.2 Delitos informáticos.

Los delitos informáticos son definidos como: “Aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información cuya consecuencia sea el daño directo o indirecto en ellos así como el mal uso de éstos” [Muñoz 2009].

A continuación se revisaran algunos de los delitos informáticos más comunes.

- **Fraude mediante el uso de la computadora y manipulación de la información que estas contienen.**

  Dispuesto en el Artículo 231fraccion XIV del Código Penal para el D.F.

  Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

  La sanción para este delito es:

  I. De veinticinco a setenta y cinco días multa, cuando el valor de lo defraudado no exceda de cincuenta veces el salario mínimo, o no sea posible determinar su valor;

  II. Prisión de cuatro meses a dos años seis meses y de setenta y cinco a doscientos días multa, cuando el valor de lo defraudado exceda de cincuenta pero no de quinientas veces el salario mínimo;

  III. Prisión de dos años seis meses a cuatro años y de doscientos a quinientos días multa, cuando el valor de lo

defraudado exceda de quinientas pero no de cinco mil veces el salario mínimo;

IV. Prisión de cuatro a seis años y de quinientos a ochocientos días multa, cuando el valor de lo defraudado exceda de cinco mil pero no de diez mil veces el salario mínimo; y

V. Prisión de seis a once años y de ochocientos a mil doscientos días multa, cuando el valor de lo defraudado exceda de diez mil veces el salario mínimo.

- **Acceso no autorizado a sistemas o servicios y destrucción de programas o datos.**

  Dispuesto en el Código Penal Federal, Artículos 211 Bis 1 al 211 Bis 7.

  Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida 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 pérdida 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 pérdida 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 pérdida 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 pérdida 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.

Es en este artículo donde se encuentra que la información es un bien jurídico siempre y cuando se encuentre almacenado en sistemas o equipos de informática que cuenten con algún mecanismo de seguridad.

El código penal federal protege la información de: modificación, copia, provocación de pérdida, destrucción y conocimiento con acceso autorizado y sin acceso autorizado. Es importante tener claro que es lo que se entiende por cada uno de estos conceptos, por lo cual se hará una pequeña descripción de cada uno de los conceptos.

Modificación: el llevar a cabo cambo en la información, los cuales no generen un daño en el contexto y que no provoque consecuencias económicas o civiles.

Copia: Es cuando la información se duplica en cualquier medio, entendiéndose como medio cualquier soporte material o electrónico.

Provocación de pérdida: Cuando de manera dolosa o por imprudencia se provoca la desaparición de información, generando daños económicos y civiles.

Destrucción: Se refiere a actividades que modifican los datos provocando un daño en todo el contexto de la información y generan daños económicos y civiles.

Conocimiento: Es cuando la persona que realiza la acción lee u observa información contenida en un medio electrónico.

A los sujetos a los que protege este artículo son: Particulares, estado, sistema financiero. Los sujetos particulares son cualquier persona física o moral que no forme parte de la esfera pública gubernamental en el momento de ser víctima.

Los sujetos englobados en el estado son cualquier persona física o moral que forma parte de la esfera pública gubernamental en el momento de ser víctima.

Dentro del sistema financiero se encuentran las instituciones de crédito, de seguros y de finanzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, unidades de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondo de retiro y cualquier otro intermediario financiero cambiario.

A continuación se muestran 3 tablas en donde se resume lo dispuesto en el artículo 211 Bis 1 al 211 Bis 7. Cada una de las tablas contiene un tipo de delito mostrando los sujetos protegidos, la sanción por cometer dicho delito y el fundamento legal en el que se puede encontrar lo dispuesto en el Código Penal Federal *(Véase tabla 2.9, 2.10 y 2.11).*

Tabla 2.9 Modificación, destrucción y provocación de perdida con acceso no autorizado.

Modificación - Destrucción – Provocación de pérdida Acceso no autorizado		
Sujeto protegido	**Sanción**	**Fundamento Legal**
Particular	6 meses a 2 años de prisión y 100 a 300 días de SMGV	211- Bis-1, primer párrafo
Estado	1 a 4 años de prisión y 200 a 600 días de SMGV	211-Bis-2, primer párrafo
Sistema Financiero	6 meses a 4 años de prisión y 100 a 600 días de SMGV	211-Bis-4, primer párrafo

Tabla 2.10 Conocimiento y copia con acceso no autorizado.

Conocimiento – Copia Acceso no autorizado		
Sujeto protegido	**Sanción**	**Fundamento Legal**
Particular	3 meses a 1 año de prisión y 50 a 150 días de SMGV	211-Bis-1, segundo párrafo
Estado	6 a 2 años de prisión y 50 a 300 días de SMGV	211-Bis-2, segundo párrafo
Sistema Financiero	3 meses a 2 años de prisión y 50 a 300 días de SMGV	211-Bis-4,segundo párrafo

Tabla 2.11 Modificación, destrucción y provocación de pérdida con acceso autorizado.

Modificación – Destrucción – Provocación de pérdida Acceso autorizado		
Sujeto protegido	**Sanción**	**Fundamento Legal**
Particular	2ª 8 años de prisión y 300 a 900 días de SMGV	211-Bis-3,primer párrafo
Sistema Financiero	6 meses a 2 años de prisión y 100 a 600 días de SMGV 50% adicional para empleados	211-Bis-4,primer párrafo

- **Acceso ilícito a equipos y medios electrónicos del sistema bancario.**

  Articulo adicionado a la reforma legislativa del 26 de junio de 2008 de la ley federal contra la delincuencia organizada, articulo 112- Quarter. Se sancionara aquel que acceda a los equipos o medios, ópticos o de cualquier otra tecnología del sistema bancario mexicano para obtener recursos económicos, información confidencial o reservada, o altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos para obtener recursos económicos, información confidencial o reservada.

  Este delito se considera grave y se castiga con prisión de tres a nueve años y de treinta mil a trescientos mil días multa.

- **Destrucción de información crediticia.**

  Dispuesta en la ley federal contra la delincuencia organizada, artículo 113. Se sancionara a los consejeros, funcionarios o empleados de las instituciones de crédito o quienes intervengan directamente en el otorgamiento de crédito que destruya u

ordene que se destruyan total o parcialmente, los sistemas o registros contables o la documentación soporte, información, documentos o archivos incluso electrónicos.

Este delito se será sancionado con prisión de dos a diez años y multa de quinientos a cincuenta mil días de salario.

- **Revelación o transmisión de información.**

Se enfoca principalmente a la protección de información sujeta a confidencialidad. Dispuesta en la ley de mercado de valores, articulo 380. Sera sancionado todo aquel que estando obligado legal o contractualmente a mantener confidencialidad, reserva o secrecía, proporcione por cualquier medio o transmita información privilegiada a otra u otras personas.

Este delito se castiga con prisión de dos a seis años.

- **Sustracción o utilización de claves de acceso.**

Delito enfocado al uso o sustracción de claves de acceso de los sistemas. Dispuesta en la ley de mercado de valores, articulo 384. Sera sancionado todo aquel que, sin consentimiento del titular sustraiga o utilice claves de acceso al sistema de recepción de órdenes y asignación de un intermediario del mercado de valores o a los sistemas operativos de negociación de las bolsas de valores, para ingresar posturas y realizar operaciones obteniendo un beneficio para si o para un tercero.

Este delito se castiga con prisión de seis meses a dos años

- **Reproducción no autorizada de programas informáticos.**

  Regulada en la Ley Federal del Derecho de Autor, artículo 11 que establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que están los programas de cómputo. La reproducción queda protegida a favor del autor y se prohíbe la fabricación o uso de sistemas o productos destinados a eliminar la protección de los programas.

  El Código Penal Federal tipifica y sanciona esta conducta con prisión de dos a diez años y de dos mil a veinte mil días de multa.

- **Uso no autorizado de programas y de datos.**

  La Ley Federal del derecho de Autor, en sus artículos 107 al 110 protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan creaciones intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de autoridades encargadas de la procuración e impartición de justicia, la información privada de las personas contenida en bases de datos no podrá ser publicada, divulgada, transmitida ni reproducida salvo con el consentimiento de la persona de que se trate.

- **Fabricación de cracks.**

  El artículo 424- Bis del Código penal federal sanciona a quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Este delito se castiga con prisión de tres a diez años y de dos mil a veinte mil días multa.

- **Denegación de servicio.**

El artículo 167 del código penal federal establece que se sancionara al que dolosamente o con fines de lucro, interrumpa p interfiera las comunicaciones, alambricas, inalámbricas o de fibra óptica, sean telegráficas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos.

Este delito se castiga con uno a cinco años de prisión y de cien a diez mil días multa.

- **Intervención de comunicaciones privadas.**

Se sanciona en el artículo 177 del código penal federal a quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente.

Este delito se sanciona de seis a doce años de prisión y de trescientos a seiscientos días multa.

- **Revelación de información obtenida en la intervención de comunicaciones privadas.**

  En el artículo 211-Bis del código penal federal se sanciona a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada.

  Se le aplicaran sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

- **Intervención de correo electrónico.**

  El articulo 167 fr.VI del Código Penal Federal sanciona con uno a cinco años de prisión y cien a diez mil días de 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. Aquí tipificaría el interceptar un correo antes de que llegue a su destinatario, pero no el abrir el buzón o los correo una vez recibidos.

- **Uso ilícito de obras.**

  El artículo 424 del código penal federal castiga a quien use en forma dolosa, con fin de lucro y son la autorización correspondiente obras protegidas por la ley federal del derecho de autor.

Este delito se castiga con prisión de seis meses a seis años y de trescientos a tres mil días multa.

- **Obtención de información que pasa por el medio**

  Este tipo de conductas que se refiere a interceptar datos que las personas envían a través de la red se tipifican en el artículo 167 fr. VI del Código Penal Federal al que se hizo referencia en el inciso anterior.

  Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos.

  Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa.

Ahora que se conocen los objetivos, actividades y retos que presenta la ciencia de cómputo forense se realizara en el siguiente capítulo un análisis comparativo de las principales metodologías para la realización de una investigación formal.

Capítulo Tercero

Análisis comparativo de metodologías forenses.

Cada año el número de crimines digitales crece, en ellos se puede apreciar un constante desarrollo de técnicas para vulnerar el sistema, así como el uso de los nuevas tecnologías. Para poder reaccionar ante estos crímenes se necesita contar con procedimientos bien definidos de cómo llevar a cabo una investigación de cómputo forense y reglas legales que permitan la penalización de estos.

En este capítulo se hará un análisis comparativo de las principales metodologías forense que existen, resaltando las ventajas que proporcionan y sus debilidades.

1. Metodologías forenses.

Dentro del cómputo forense no existe una metodología universal de cómo llevar a cabo una investigación, sin embargo existen algunas metodologías bien conocidas y muchas guías de buenas prácticas que se centran en cómo realizar alguna de las actividades que se llevan a cabo en una investigación de cómputo forense sobre algún sistema operativo o dispositivo en específico.

Con el desarrollo acelerado de la tecnología encontramos un gran número de dispositivos de cómputo que son utilizados como parte de las actividades diarias de un individuo. Cada individuo almacena comparte y produce información digital en estos dispositivos.

Este crecimiento acelerado en el número de dispositivos y el uso desmesurado de ellos dentro de las actividades diarias no es el único problema, sino que cada uno de estos dispositivos cuenta con una forma de operación, un software y hardware distinto.

Por lo cual no basta con contar con técnicas y herramientas que ayuden a la preservación, análisis y presentación de la evidencia, se necesita contar con metodologías que se puedan aplicar a todos y cada uno de los dispositivos que se encuentren dentro de una escena del crimen, proporcionando el procedimiento correcto para llevar la investigación a un resultado satisfactorio.

A continuación se revisaran las principales metodologías forenses, describiendo groso modo cada una de sus etapas o fases.

1.1 Metodología del Instituto SANS.

Existe una metodología que es la más difundida dentro del ámbito forense y es la metodología presentada por el SANS Institute[19] (instituto SANS). A continuación se muestra el esquema de su metodología. *(Veáse fig. 3.1).*

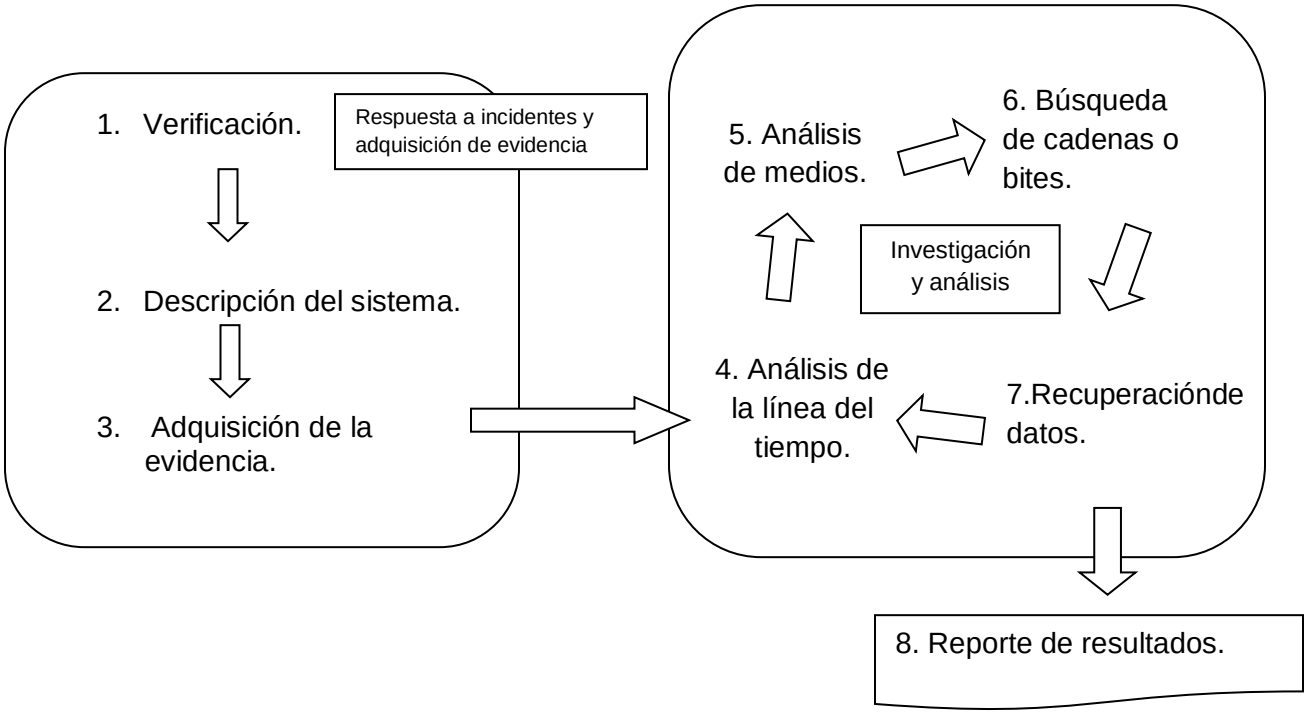


Figura 3.1. Metodología propuesta por el Instituto SANS.

Esta metodología consta de ocho pasos que son: la verificación, la descripción del sistema, la adquisición de la evidencia, el análisis de la línea de tiempo, el análisis de medios, la búsqueda de cadenas o bites, la recuperación de

[19] Establecida como una cooperativa en la investigación y la organización de la educación. Es una de las instituciones que ofrece certificaciones en seguridad y pone a disposición sin costo alguno una colección de documentos de investigación sobre diversos aspectos de seguridad de la información.

datos y el reporte de resultados. Con estos ocho pasos se abarcan las cuatro etapas principales del cómputo forense –identificación, preservación, análisis y presentación.

1 *Verificación.* Es el primer paso que se debe hacer siguiendo esta metodología. El objetivo en este paso es asegurarse de que un incidente ha tenido lugar.

2 *Descripción del sistema.* De haberse detectado un incidente entonces de realizará este segundo paso en donde se hará la descripción del tipo de sistemas operativos y el rol que juegan en estos sistemas dentro de la red.

3 *Adquisición de la evidencia.* En este paso se requiere la presencia de un investigador o analista forense que se encargará de hacer la adquisición de evidencia volátil y no volátil del sistema.

4 *Análisis de la línea de tiempo.* Ya dentro de la etapa del análisis la metodología indica que se debe realizar la línea del tiempo en la cual se debe de incluir el día y la fecha en la que se realizaron las modificaciones, accesos y cambios o creaciones de todos los archivos en los que se encuentre evidencia.

5 *Análisis de medios.* En este paso el investigador deberá recolectar la información derivada de la investigación hecha dentro de los archivos seleccionados del sistema.

6 *Búsqueda de cadenas o bytes.* Es en este paso donde se hará la búsqueda de palabras claves dentro de los archivos. Las palabras claves son aquellas palabras que se han ido recolectando a lo largo de la investigación y que dan alguna pista de lo que estamos buscando. Una palabra clave puede ser el nombre de una persona, una dirección de correo, una dirección IP, una hora, etc.

7 *Recuperación de datos.* Este es el paso donde el analista deberá hacer la recuperación y análisis de la información que ha encontrado como resultado del análisis previamente hecho. Una vez recuperados los datos éstos deben ser colocados en la línea de tiempo.

8 *Reporte de resultados.* Este es el paso final de esta metodología. En él se realizará la creación del reporte donde se detallará la investigación que se llevó a cabo siguiendo los pasos anteriores y el resultado obtenido del análisis.

A continuación se muestra una tabla con todos los pasos que propone la metodología SANS y los pasos generales de una investigación forense, enfatizando la correspondencia entre ellos *(Véase tabla 3.1).*

Tabla 3.1 Pasos de la metodología SANS ubicados en las etapas generales de una metodología forense.

Etapas generales de una investigación forense	**Pasos de la metodología SANS**							
	Verificación	Descripción del sistema	Adquisición de la evidencia	Análisis de la línea de tiempo	Análisis de medios	Búsqueda de cadenas o bites	Recuperación de datos	Reporte de resultados
Identificación	✓	✓						
Preservación			✓					
Análisis				✓	✓	✓	✓	
Presentación								✓

En esta tabla se puede ver que la metodología SANS cubre todas las etapas que se necesitan para realizar una investigación forense. Algunas de las etapas generales de la investigación forense son desarrolladas en más de un paso por la metodología SANS.

A continuación se presentan las particularidades, ventajas y desventajas que proporciona esta metodología.

Tabla 3.2 Particularidades, ventajas y desventajas de la metodología SANS.

Metodología SANS		
Particularidades	**Ventajas**	**Desventajas**
Proporciona un modelo de las formatos necesarios para establecer la cadena de custodia Define lugares en donde se puede encontrar información oculta dentro de los sistemas operativos Windows y Linux.	Cubre con todas las etapas requeridas para hacer una investigación forense. Toma en cuenta el cuidado de la cadena de custodia lo cual es un aspecto importante para que las evidencias encontradas tengan valides.	No propone métodos para realizar la adquisición de evidencia de grandes volúmenes de datos. No propone métodos de análisis para volúmenes grandes de datos. Está diseñada para ser aplicada en investigaciones donde los dispositivos involucrados sean sólo computadoras que cuenten con sistemas operativos Windows o Linux. Esto deja fuera la posibilidad de que se pueda aplicar está metodología en dispositivos como lo son los teléfonos celulares y tabletas electrónicas que ahora es tan común encontrar involucrados dentro de un incidente de seguridad.

1.2 Metodología de Análisis Forense Digital del laboratorio de Cibercrimen del departamento de justicia de E.U.A.

Otra de las metodologías importantes dentro del cómputo forense es la metodología propuesta por el Laboratorio de cibercrimen del Departamento de Justicia (DOJ) de los Estados Unidos de América que propone una metodología de tres etapas: la preparación y extracción, la identificación y el análisis *(Véase fig. 3.2).*

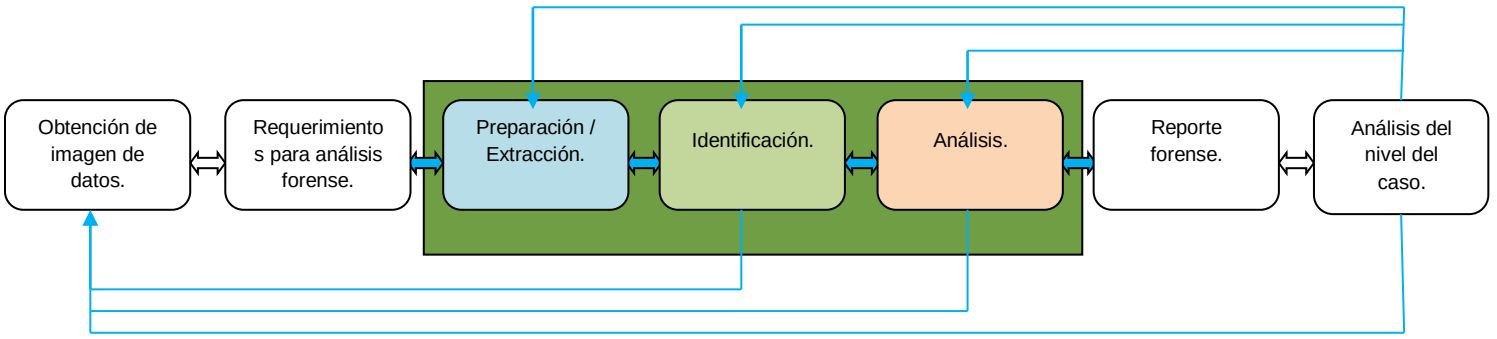


Figura 3.2. Etapas principales propuestas en la metodología del Departamento de Justicia de los Estados Unidos de América.

1. Dentro de la etapa de *preparación / extracción* se realiza la configuración necesaria para hacer la duplicación de los datos, la duplicación y posteriormente la verificación de integridad de datos.

   Para poder realizar esta etapa, el analista debe contar previamente con la información necesaria para empezar el proceso de duplicación. La información con la que debe de contar es: saber cuál es el dispositivo del cual hará la extracción de datos y que datos son lo que necesita extraer.

   La etapa finalizará cuando se halla extraído toda la información requerida, entonces se podrá avanzar a la siguiente etapa de identificación.

2. En la etapa de *identificación* se buscará dentro de la imagen obtenida en la etapa de preparación/extracción información relevante al caso. Esto se hace mediante una lista de búsqueda en donde se tiene especificado el tipo de información que se espera encontrar o bien el lugar donde se espera encontrar la evidencia. Puede ser que mientras se desarrolla la búsqueda de la información que ya se tiene en esta lista surjan nuevos lugares o información que se crea conveniente agregar a la lista para realizar su búsqueda.

   Esta etapa no terminará hasta que se haga la búsqueda de toda la información que se encuentra en la "lista de búsqueda".

   Una vez que se tengan localizados los lugares que contienen evidencia del caso se podrá pasar a la siguiente etapa: el análisis.

3. La etapa del *análisis* es la última etapa que describe esta metodología, en ella se realizará el análisis de la información que previamente se seleccionó. Se buscará conocer todos sus detalles como lo son:

   - Por qué aplicación fueron creados, modificados, enviados o recibidos.
   - De dónde proceden.
   - Cuándo fueron creados accedidos, modificados, recibidos, enviados, vistos o borrados. Estos datos se deberán colocar en una línea de tiempo que permita ver qué fue lo que sucedió en el sistema y cuándo.
   - Cómo fue originado en el medio, cómo fue creado, modificado, transmitido y usado.
   - Encontrar información que lo asocie con registros del sistema, bitácoras de aplicaciones y bitácoras de sistema.

Una vez que se cuente con toda esta información se empezará el reporte forense.

A continuación se muestra el diagrama completo de la metodología en donde se describe cada una de las etapas de la metodología *(Véase fig. 3.3).*

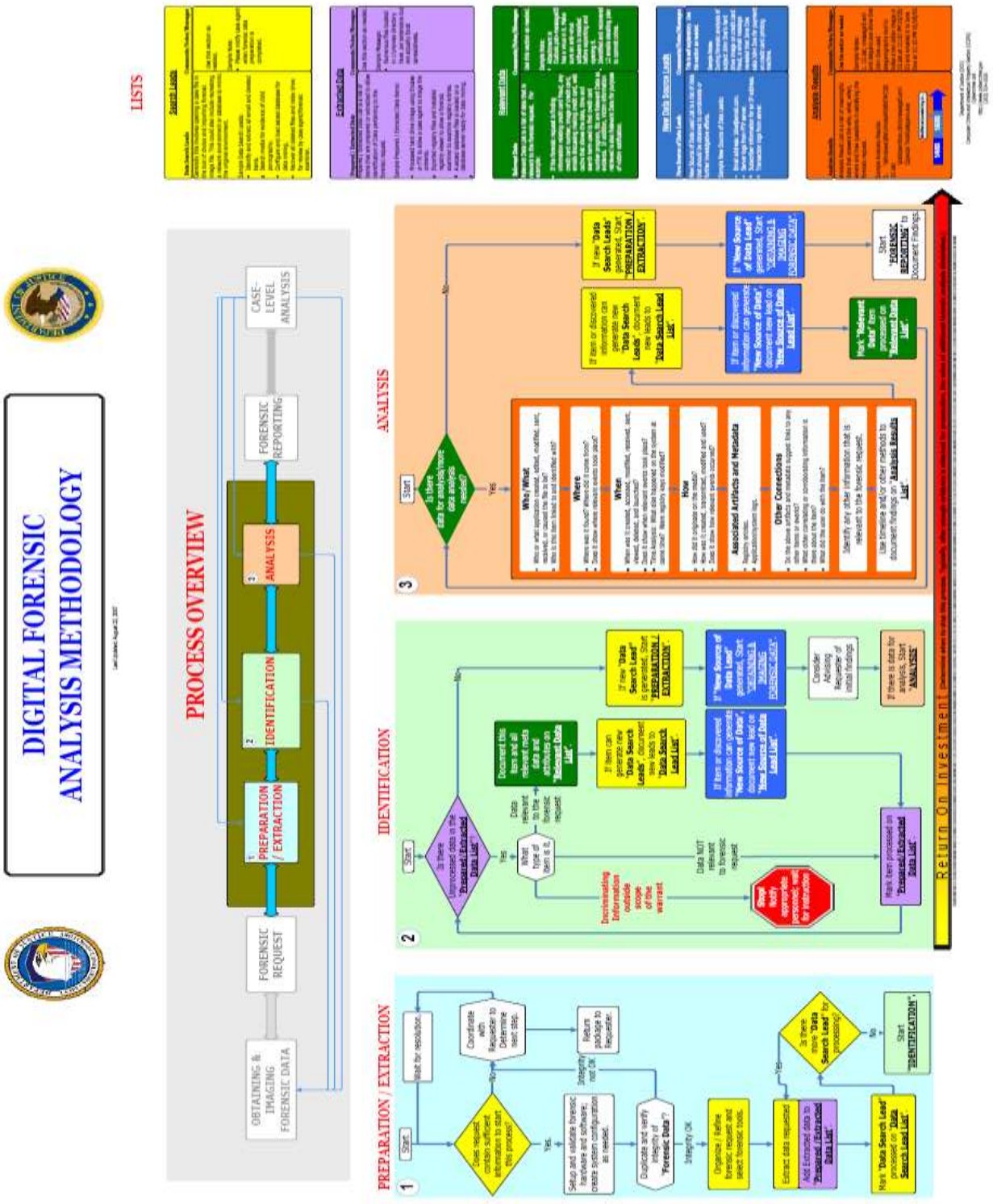


Figura 3.3. Metodología del Laboratorio de cibercrimen del Departamento de Justicia de los Estados Unidos de América.

A continuación se muestra una tabla con todos los pasos que propone esta metodología y los correspondientes con los pasos generales de una investigación forense *(Véase tabla 3.3)*

Tabla 3.3 Pasos de la metodología DOJ ubicados en las etapas generales de una metodología forense.

Etapas generales de una investigación forense	**Pasos de la metodología DOJ**		
	Preparación/Extracción	Identificación	Análisis
Identificación			
Preservación	✓		
Análisis		✓	✓
Presentación			

Como se puede ver en la tabla 3.3 la metodología DOJ sólo cubre dos de las cuatro etapas que se deben realizar en una investigación forense. Las etapas que cubre son: la preservación y el análisis, dejando fuera la identificación y la presentación fases fundamentales para la realización de una investigación forense.

A continuación se presentan las particularidades, ventajas y desventajas que proporciona esta metodología *(Véase tabla 3.4)*.

Tabla 3.4 Particularidades, ventajas y desventajas de la metodología DOJ.

Metodología DOJ		
Particularidades.	**Ventajas.**	**Desventajas.**
Especifica un flujo bien definido para la realización de cada una de las etapas que propone.	Seguir los pasos propuestos en esta metodología es muy fácil ya que es muy claro el procedimiento que se debe de seguir gracias al diagrama de flujo que proporciona para cada una de las etapas.	No cubre las etapas generales necesarias para realizar una investigación forense. Esta metodología está enfocada a la investigación de computadoras que cuenten con un sistema operativo Windows. Esto provoca que en muchos casos esta metodología no pueda ser aplicada. No propone metodologías para realizar análisis en grandes volúmenes de información. No se establece una cadena de custodia en ninguna de las etapas propuestas. No da resultados para el progreso del sistema.

1.3 Metodología del Grupo de Trabajo de Investigación Forense Digital.

Esta es una metodología desarrollada por el grupo de trabajo de investigación forense digital (Digital Forensics Research Workshop DFRW). Esta metodología consta de siete etapas que son: la identificación, la preservación, la recolección, la examinación, el análisis, la presentación y la decisión.

Para seis de las siete etapas definidas en esta metodología, se proponen actividades a realizar, estas actividades se encuentran agrupadas en una tabla *(Véase tabla 3.5)*.

Tabla 3.5 Etapas y procesos de la metodología del DFRW.

Identificación	Preservación	Recolección	Examinación	Análisis	Presentación	Decisión
Evento/detección del crimen	Manejo del caso	Preservación	Preservación	Preservación	Documentación	
Acuerdo de firma	Tecnologías de imagen	Métodos aprobados	Recabar pistas	Trazabilidad[20]	Testimonio de expertos	
Detección del perfil	Cadena de custodia	Software aprobado	Técnicas de validación	Estadístico	Aclaración	
Detección de anomalías	Sincronización del tiempo	Hardware aprobado	Técnicas de filtración	Protocolos	Misión de la declaración de impacto	
Quejas		Autoridad legal	Igualar patrones	Minería de datos	Recomendación de contramedidas	
Monitoreo del sistema		Compresión sin perdidas	Descubrimiento de datos ocultos	Línea de tiempo	Interpretación estática	
Auditoria del análisis		Toma de muestras	Extracción de datos ocultos	Enlaces		
Etc.		Técnicas de recuperación		Espacial		

[20]Por trazabilidad se entiende el descubrimiento de la causa u origen de algo derivado de la examinación realizada. Encontrar evidencia de algo que ha pasado.

A continuación se describirá cada una de estas seis etapas.

1. *Identificación.* En esta etapa se busca tener la certeza de que el incidente ocurrió para lo cual se proponen actividades como detectar las anomalías, revisar el monitoreo del sistema, analizar las auditorias entre otras.

2. *Preservación.* En esta etapa se busca mantener la integridad de los datos. Para ello propone implementar tecnología para realizar las imágenes, sincronizar los tiempos y establecer la cadena de custodia.

3. *Recolección.* La recolección tiene como objetivo la recuperación de todos los datos en los que se pueda encontrar evidencia que resuelva las preguntas ¿Quién?, ¿Cómo?, ¿Cuándo? Para lo cual se propone implementar las técnicas adecuadas de preservación de los datos, aprobar métodos, aprobar software y hardware, obtener la autorización legal y aplicar técnicas de recuperación.

4. *Examinación.* Para realizar la examinación es necesario implementar técnicas para conservar la integridad de los datos –técnicas de preservación- Además de ligar la información, implementar filtros, ligar patrones, descubrir datos ocultos y hacer la extracción de los datos ocultos.

5. *Análisis.* Para realizar el análisis se hace necesario la implementación de técnicas de preservación para que aun con las técnicas de análisis que se apliquen a los datos éstos no se vean alterados de ninguna manera. Las actividades propuestas para realizar el análisis de datos son: ligar los eventos encontrados, realizar análisis estadístico, realizar minería de datos, realizar una línea de tiempo, entre otras.

6. *Presentación.* El objetivo de esta etapa es dar a conocer los resultados de la investigación así como el procedimiento que se siguió durante la

investigación para poder llegar a esos resultados. Para lo cual se hace la documentación de la investigación, se agrega el testimonio de expertos, interpretación de estadísticas y recomendación de contramedidas.

A continuación se muestra una tabla con todos los pasos que propone esta metodología y so correspondencia con los pasos generales de una investigación forense *(Véase tabla 3.6).*

Tabla 3.6 Pasos de la metodología DFRW ubicados en las etapas generales de una metodología forense.

Etapas generales de una investigación forense	**Pasos de la metodología DFRW**						
	Identificación	Preservación	Recolección	Examinación	Análisis	Presentación	Decisión
Identificación	✓	✓					
Preservación			✓				
Análisis				✓	✓		
Presentación						✓	

A continuación se presentan las particularidades, ventajas y desventajas que proporciona esta metodología *(Véase tabla 3.7)*.

Tabla 3.7 Particularidades, ventajas y desventajas de la metodología DFRW.

Metodología DFRW		
Particularidades	**Ventajas.**	**Desventajas.**
Provee una lista de los lugares más comunes en los que se puede encontrar información oculta. Provee métodos y actividades para la localización de información oculta.	Cubre con todas las etapas requeridas para hacer una investigación forense. Construye una metodología que define todo el universo de dispositivos y plataformas que puedan ser analizadas dentro de una investigación de cómputo forense. Enfocada a conservar la integridad y mantener la cadena de custodia de los datos durante todo el proceso de la investigación, para que pueda ser aceptada en una corte legal. Considera para el análisis el empleo de técnicas para la extracción de datos ocultos. Considera métodos para el análisis de grandes volúmenes de información. Es una metodología que se encuentra en constante actualización.	No propone un procedimiento específico para la realización de las actividades.

1.4 Metodología de Kevin Mandia y Chris Prosise.

Esta metodología busca organizar las fases de un procedimiento de respuesta a incidentes. Dentro del procedimiento marcado para reaccionar ante un incidente se describe el procedimiento para realizar la investigación del incidente, es por ello que se toma en cuenta dentro de este análisis de metodologías de cómputo forense.

Esta metodología se compone de siete etapas que son: la pre-preparación de incidentes, la detección de incidentes, la respuesta inicial, la formulación de una estrategia de respuesta, la investigación del incidente, el reporte y la resolución *(Véase fig. 3.4).*

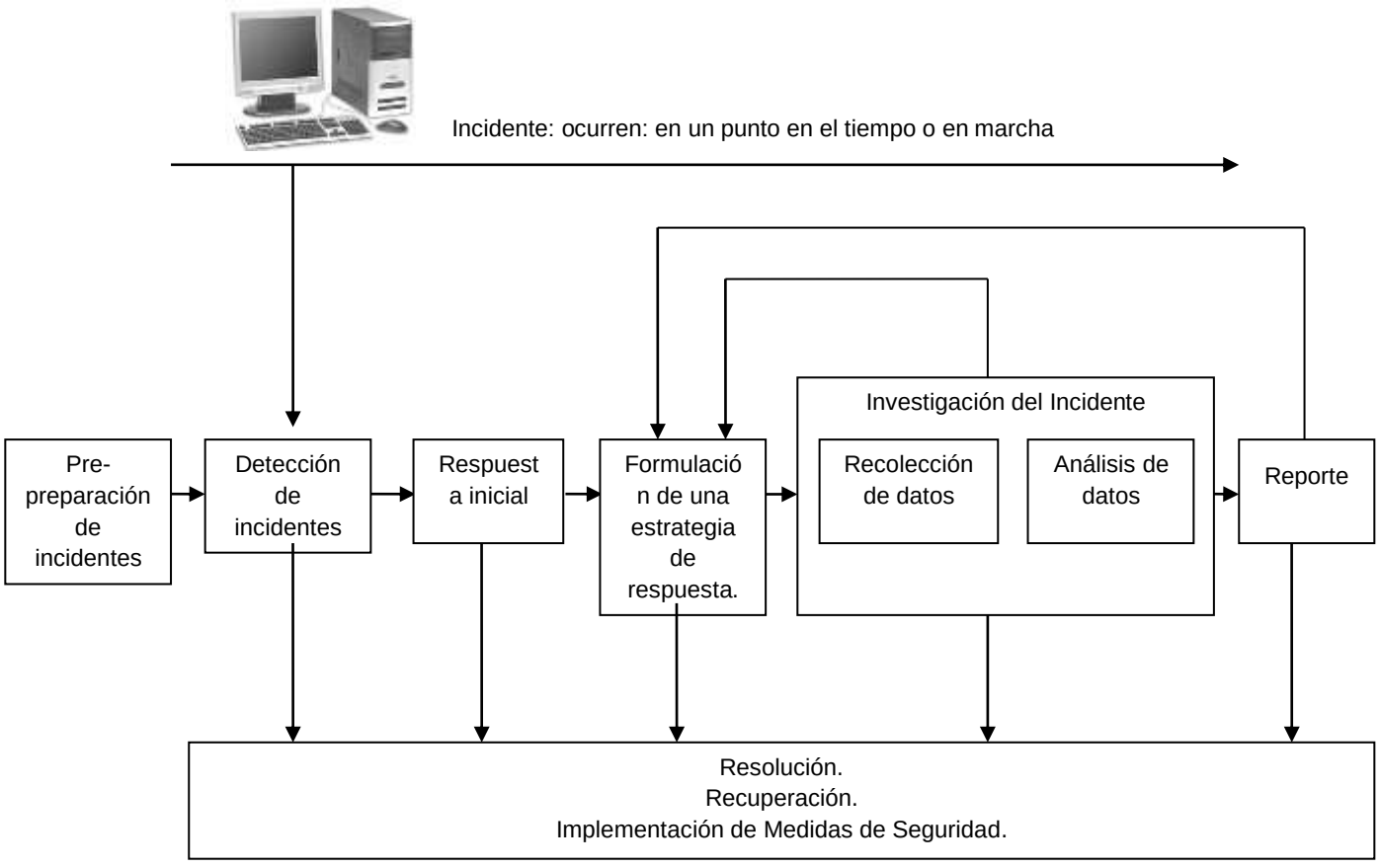


Figura 3.4. Metodología de Kevin Mandia y Chris Prosise.

En la etapa de *pre-preparación de incidentes se* engloban todas las acciones pertinentes para preparar a la organización y al equipo encargado de reaccionar ante un incidente, además de preparar las herramientas que se necesitaran.

En la etapa de *detección de incidentes* se realiza la identificación de los incidentes potenciales en seguridad computacional dependiendo de los equipos e infraestructura que se tiene.

Dentro de la etapa de *respuesta inicial* se lleva a cabo el inicio de la investigación, registrando todos los detalles al que rodean al incidente, se hace la reunión del equipo de respuesta a incidentes y se notifica a las personas que necesitan saber del incidente.

Seguida a esta etapa se encuentra la etapa de *formulación de una estrategia de respuesta* en donde con base en los resultados de todos los hechos que se conocen se determinara la mejor respuesta, esta respuesta tendrá que ser aprobada por la directiva.

Se regresara a esta etapa una vez que se haya llevado a cabo la investigación del incidente para determinar las acciones civiles, penales, administrativas o de otra índole que sea apropiado tomar, esto con base a las conclusiones obtenidas de la investigación.

La etapa de *investigación del incidente* se encuentra dividida en dos sub etapas: la recolección de datos y el análisis de los datos. En esta etapa de investigación del incidente se realizará la colección completa de datos, estos datos serán analizados para determinar que ocurrió, cuándo ocurrió, quién lo hizo y cómo se puede prevenir en el futuro.

La etapa del *reporte* es en donde se deberá comunicar con precisión toda la información acerca de la investigación. Este reporte deberá ser escrito de forma tal que sea útil a las personas encargadas de tomar decisiones.

Por último en esta metodología se encuentra la etapa de *resolución* en la cual se busca emplear medidas de seguridad y cambios en los procedimientos. Así como llevar un registro de las lecciones aprendidas y desarrollar soluciones a largo plazo para los problemas identificados.

Esta es una metodología que aunque no es una metodología forense sino de respuesta a incidentes, cubre con todas la etapas de una investigación forense e incluye algunas prácticas como la pre- preparación que en ninguna otra metodología se había visto.

A continuación se muestra una tabla con todos los pasos que propone esta metodología contraponiéndolos con los pasos generales de una investigación forense *(Véase tabla 3.8).*

Tabla 3.8 Pasos de la metodología Kevin Mandia y Chris Prosise ubicados en las etapas generales de una metodología forense.

Etapas generales de una investigación forense	**Pasos de la metodología Kevin Mandia y Chris Prosise**						
	Pre-preparación	Detección de incidentes	Respuesta inicial	Formulación de una estrategia de	Investigación de incidentes	Reporte	Resolución
Identificación		✓	✓				
Preservación				✓	✓		
Análisis					✓		
Presentación						✓	

A continuación se presentan las particularidades, ventajas y desventajas que proporciona esta metodología *(Véase tabla 3.9)*.

Tabla 3.9 Particularidades, ventajas y desventajas de la metodología Kevin Mandia y Chris Prosise.

Metodología Kevin Mandia y Chris Prosise		
Particularidades	**Ventajas**	**Desventajas**
Propone un paso llamado pre-preparación en el cual el grupo encargado de reaccionar ante un incidente se anticipa a ellos preparando las herramientas necesarias y conocimientos de la infraestructura. Proporciona una lista de los principales ataques que se presentan hacia una computadora y recomienda una estrategia de respuesta.	Cumple con todas las etapas generales de una investigación forense. Proporciona métodos para realizar el análisis de datos.	No propone métodos para el análisis de grandes volúmenes de información Está enfocada a para la investigación de plataformas Windows NT/2000, UNIX y routers Cisco. Dejando fuera todos los dispositivos que utilicen una plataforma diferente.

1.5 Análisis comparativo.

Se han revisado cuatro metodologías en las que se proponen diferentes procedimientos para realizar una investigación forense. Las dos primeras metodologías –la metodología propuesta por el SANS y la metodología propuesta por el laboratorio de cibercrimen del departamento de justicia de los Estados Unidos de América- están enfocadas a la realización de una investigación forense en computadoras con Windows o Linux.

Centrar una metodología en algún tipo de dispositivo o plataforma hace que esta no sea aplicable en todos los casos en los que se necesite realizar una investigación forense.

Se puede entender que hace unos años pensar en datos almacenados en forma digital nos remontara a una computadora pero ahora ya no es así, existe un sinfín de dispositivos que almacenan información en forma digital para los cuales estas dos metodologías no podrían ser aplicadas.

Una de las metodologías que propone un modelo que no está enfocado en ningún dispositivo ni plataforma es la metodología propuesta por el grupo de trabajo de investigación forense digital

Esa característica es importante encontrarla en una metodología de investigación forense ya que brinda la posibilidad de ser aplicarla en todos los dispositivos y plataformas que se encuentren involucrados en el incidente, adecuando las actividades a las necesidades que el caso presente.

También se puede notar que existen metodologías que no cubren las etapas principales que conlleva una investigación forense como lo es la metodología del laboratorio de cibercrimen del departamento de justicia de los Estados Unidos de América *(Véase tabla 3.10).*

Tabla 3.10 Etapas de una investigación de cómputo forense localizadas en las diferentes metodologías.

Etapas de la investigación.	Metodologías.			
	SANS	DOJ	DFRW	Kevin Mandia y Chris Prosise
Identificación	✓	✓		✓
Recolección	✓	✓	✓	✓
Análisis	✓	✓	✓	✓
Presentación	✓	✓		✓

El no cubrir con alguna de las etapas principales de la investigación forense deja el proceso inconcluso o deja una vaga idea de que actividades se deben de realizar para poder cumplir con las etapas faltantes.

Si no se cuentan con los procedimientos suficientes para realizar todas las etapas de una investigación forense lo más probable es que el resultado no sea el esperado o que si la investigación requiere ser presentada ante una corte legal no cumpla con los requerimientos necesarios y las pruebas sean desechadas, causando así la omisión de la evidencia hallada en los sistemas de cómputo que pudiera ser relevante al caso.

De la última metodología revisada se debe destacar el modelo que propone ya que aunque este no está dirigido a hacer investigación forense contiene un paso clave que es la pre-preparación en donde se previenen las herramientas, habilidades y equipo que se necesitara para poder responder ante un incidente de seguridad. Además de prever las amenazas potenciales que tiene un sistema de información.

Esto definitivamente marcará la diferencia en el momento de enfrentarse a la investigación forense de un sistema, ya que se cuenta con información y herramientas anticipadas al incidente.

A continuación en la figura 3.5, se resume cada una de las metodologías donde se podrán ver las etapas que cada una propone sus particularidades, ventajas y desventaja.

Metodología SANS

Particularidades	Ventajas	Desventajas
Proporciona un modelo de las formatos necesarios para establecer la cadena de custodia Define lugares en donde se puede encontrar información oculta dentro de los sistemas operativos Windows y Linux.	Cubre con todas las etapas requeridas para hacer una investigación forense. Toma en cuenta el cuidado de la cadena de custodia lo cual es un aspecto importante para que las evidencias encontradas tengan valides.	No propone métodos para realizar la adquisición de evidencia de grandes volúmenes de datos. No propone métodos de análisis para volúmenes grandes de datos. Está diseñada para ser aplicada en investigaciones donde los dispositivos involucrados sean sólo computadoras que cuenten con sistemas operativos Windows o Linux. Esto deja fuera la posibilidad de que se pueda aplicar está metodología en dispositivos como lo son los teléfonos celulares y tabletas electrónicas que ahora es tan común encontrar involucrados dentro de un incidente de seguridad.

Metodología DOJ

Particularidades.	Ventajas.	Desventajas.
Especifica un flujo bien definido para la realizacion de cada una de las etapas que propone.	Seguir los pasos propuestos en esta metodologia es muy fácil ya que es muy claro el procedimiento que se debe de seguir gracias al diagrama de flujo que proporciona para cada una de las etapas.	No cubre las etapas generales necesarias para realizar una investigación forense. Esta metodologia esta enfocada a la investigación de computadoras que cuenten con un sistema operativo Windows. Esto provoca que en muchos casos esta metodología no pueda ser aplicada. No propone metodologias para realizar analisis en grandes volúmenes de información. No se establece una cadena de custodia en ninguna de las etapas propuestas. No da resultados para el progreso del sistema.

Metodología DFRW

Particularidades	Ventajas.	Desventajas.
Provee una lista de los lugares más comunes en los que se puede encontrar informacion oculta. Provee métodos y actividades para la localizacion de informacion oculta.	Cubre con todas las etapas requeridas para hacer una investigación forense. Construye una metodología que define todo el universo de dispositivos y plataformas que puedan ser analizadas dentro de una investigación de cómputo forense. Enfocada a conservar la integridad y mantener la cadena de custodia de los datos durante todo el proceso de la investigación, para que pueda ser aceptada en una corte legal. Considera para el análisis el empleo de tecnicas para la extracción de datos ocultos. Considera métodos para el analisis de grandes volúmenes de información. Es una metodología que se encuentra en constante actualización.	No propone un procedimiento especifico para la realización de las actividades.

Metodología Kevin Mandia y Chris Prosise

Particularidades	Ventajas	Desventajas
Propone un paso llamado pre-preparación en el cual el grupo encargado de reaccionar ante un incidente se anticipa a ellos preparando las herramientas necesarias y conocimientos de la infraestructura Proporciona una lista de los principales ataques que se presentan hacia una computadora y recomienda una estrategia de respuesta.	Cumple con todas las etapas generales de una investigación forense. Proporciona métodos para realizar el análisis de datos.	No propone métodos para el análisis de grandes volúmenes de información Está enfocada a para la investigación de plataformas Windows NT/2000, UNIX y routers Cisco. Dejando fuera todos los dispositivos que utilicen una plataforma diferente.

Figura 3.5 Síntesis de las metodologías analizadas.

Al buscar una metodología de cómputo forense que ayude al analista a realizar una investigación, se busca que la metodología contenga: los pasos necesarios para desarrollar la investigación, funja como guía dentro del proceso de investigación proponiendo las actividades a realizar en cada uno de los casos, contenga actividades dedicadas a mantener la evidencia integra para que esta puede ser presentada ante una corte legal y resuelva los retos a los que se presenta el cómputo forense.

Los retos más grandes que presenta el cómputo forense en este momento son:

- Los usuarios de dispositivos de cómputo cada vez almacenan más información de forma digital haciendo que las imágenes forenses tomadas sean de volúmenes descomunales tanto que es imposible tener el tiempo suficiente para poder analizar toda esta información. Por lo que se requiere de nuevos métodos de análisis.

- Existen un número enorme de dispositivos de cómputo el cual no solo es grande sino que sigue creciendo y cada vez será más común encontrar estos dispositivos envueltos en la escena del crimen.

  El reto para el cómputo forense será estar actualizado a la velocidad en que estos dispositivos crecen y contar con metodologías forense que proporcionen los pasos y métodos necesarios para poder analizar cada uno de estos dispositivos.

  Es por esto que una metodología forense no puede estar dirigida sólo a un tipo de dispositivo o plataforma, pues debe cubrir el espacio de dispositivos en uso.

- Cada vez es más común que los datos clave dentro de un caso de cómputo forense se encuentren: cifrados, haciendo uso de esteganografía, en cuentas de email anónimas, en cuentas de correo falsas, proviniendo de direcciones IP suplantadas, proviniendo de direcciones MAC suplantadas y

haciendo uso de otros medios que sirvan para ocultar la verdadera identidad del criminal en el ciberespacio. Por lo que la metodología elegida para realizar la investigación de cómputo forense deberá proponer métodos para analizar este tipo de datos.

En la siguiente tabla se especifica que metodologías de las analizadas anteriormente cuentan con métodos que ayuden a superar los retos que enfrenta el cómputo forense *(Véase tabla 3.11).*

Tabla 3.11 Metodologías que consideran los retos del cómputo forense.

Retos del cómputo forense				
	SANS	DOJ	DFRW	Kevin Mandia y Chris Prosise
Cubre con todos los pasos generales para realizar una investigación de cómputo forense	✓		✓	✓
Implementación en todos los dispositivos.			✓	
Manejo de grandes volúmenes de información.			✓	
Respuesta a las técnicas para ocultar datos	✓		✓	✓

Derivado del análisis hecho de las metodologías anteriores se hace, en el siguiente capítulo, la propuesta de una metodología para la realización de una investigación de cómputo forense.

Capítulo Cuarto

Propuesta de Metodología para Realizar una Investigación Forense.

Después de analizar las metodologías más importantes dentro del campo del cómputo forense, de conocer sus aportaciones y sus deficiencias; se hace la propuesta de una metodología que conserva lo mejor de cada una de las metodologías analizadas y que responde a los retos actuales que enfrenta el cómputo forense.

Esta metodología no se encuentra dirigida hacia ningún tipo de tecnología, dispositivo, sistema operativo o plataforma. Busca ser general, para que pueda ser implementada en cualquier dispositivo. Propone actividades para analizar grandes volúmenes de datos y responder ante las técnicas de ocultamiento de información.

1. Consideraciones para la propuesta de una Metodología para Realizar una Investigación Forense.

Para conformar la metodología que a continuación se mostrará, se tomaron en cuenta las mejores propuestas hechas en las metodologías analizadas, aquellas propuestas que hacen una mejora importante a la realización de una investigación forense. Estas propuestas son extraídas para ser incluidas en esta nueva metodología.

En algunos casos estos puntos extraídos se encuentran en una fase en específico y en otros se encuentran presentes durante todo el desarrollo de las diferentes fases que conforman la metodología

Los puntos extraídos de las metodologías analizadas son tres:

- La propuesta de una etapa de prevención que se hace en la metodología de Kevin Mandia y Chris Prosise.
- La propuesta de dar métodos por cada una de las fases que se propongan en la metodología. Esta idea es tomada de la metodología DFRW.
- La propuesta de proporcionar un flujo definido en el cual se realizarán las actividades de cada una de las fases. Esta es extraída de la metodología DOJ.

En el caso del primer punto extraído - incluir un etapa de prevención- se ve incluido en la metodología dentro de la fase de prevención. Este punto se incorpora haciéndole algunas modificaciones, pues mientras que en la metodología Kevin Mandia y Chris Prosise se propone realizar en esta etapa la preparación y organización del equipo encargado de reaccionar ante un incidente, procurando la rápida restauración del sistema, en esta metodología se enfoca esta

fase en las actividades que se tienen que prever para reaccionar ante un caso de cómputo forense.

El segundo punto extraído – proporcionar métodos en cada una de las fases de la metodología- se incorpora a lo largo del desarrollo de la metodología propuesta, dando en cada una de las fases métodos que ayuden a conseguir el objetivo de cada fase.

Por último el tercer punto extraído –contar con un flujo definido en cada una de las fases- también se puede ver presente en cada una de las fases de la metodología propuesta, las cuales tienen establecido una serie de pasos consecutivos para ser desarrolladas.

Durante el análisis de las metodologías que se hizo en el capítulo tercero, al igual que se encontraron propuestas valiosas para conformar una metodología se encontraron deficiencias que vale tener presentes para evitar que la metodología propuesta las incluya.

Se encontró que en su mayoría estas metodologías se aplican a dispositivos o tecnologías en específico y que muchas de ellas no responden a los retos actuales que presenta la ciencia del cómputo forense.

Por lo que para la propuesta de la metodología se tomaron en cuenta cuatro puntos importantes:

- Que la metodología propuesta fuera una metodología general. Es decir aplicable a cualquier dispositivo de cómputo y a cualquier tecnología.
- Que fuera capaz de enfrentarse a problemas como el volumen de información que actualmente es manejado y que se encuentra en constante crecimiento.
- Que contara con un procedimiento detallado para lograr que la evidencia mostrada sea aceptable en un procedimiento legal.
- Que contara con procedimientos para tratar información oculta.

Metodología general. Para lograr que la metodología forense fuese general no se centró ningún proceso en algún dispositivo o tecnología en específico. Para poder proponer actividades a realizar en cada una de las fases de la metodología se tomaron en cuenta las características generales de los dispositivos de cómputo.

De esta manera se pudieron proponer acciones para realizar la extracción de datos, protegerlos ante posibles alteraciones de la información que almacena, y para realizar el análisis de los datos.

Metodología para grandes volúmenes de información. Para poder tratar grandes volúmenes de información se sugieren técnicas para la discriminación de información en el momento de la extracción de datos. También se sugieren técnicas para realizar el análisis en grandes volúmenes de datos. Esto se hace durante la fase de adquisición de evidencia y durante la fase de análisis.

Metodología con una descripción detallada. En cada una de las fases propuestas se marca un objetivo general de la fase, posteriormente se hace una descripción detallada de las actividades que se deben realizar, se marca el orden en el que se deben ejecutar y las herramientas que se pueden emplear.

Metodología para información oculta. Se puede observar que cada vez es más común encontrar evidencia oculta, es decir información que haya empleado técnicas para ocultar información como lo puede ser el cifrado o el uso de esteganografía.

Esta metodología dentro de la fase de análisis, hace la propuesta de actividades que ayuden a descubrir si existe algún tipo de datos que hayan hecho uso de estas técnicas para ocultar la información. De esta manera se podrá contar con toda la evidencia del caso.

Estas actividades se deben realizar con la aprobación de la autoridad correspondiente para no caer en un acto ilegal de violación de la privacidad. Este tipo de advertencias también son mencionadas durante la descripción de la metodología.

La metodología busca que todos los resultados encontrados durante el desarrollo de las diferentes fases sean mediante procesos comprobables para poder dar una versión de lo sucedido en el sistema basada en la evidencia encontrada. Y de esta manera proporcionar a la ley una fuente de confianza más que le sirva para dar su veredicto.

Por último se incluyen propuestas que no se encuentran en ninguna de las metodologías analizadas con anterioridad y que sin embargo resulta importante incluirlas para poder tener una investigación forense exitosa.

Las propuestas nuevas incluidas son:

- La devolución de evidencia a la entidad una vez que el proceso ha terminado.
- La eliminación segura de evidencia.
- La propuesta de herramientas que se puedan utilizar en cada una de sus fases.
- La especificación de un objetivo para cada una de las fases que conforman la metodología.

A continuación se muestra una tabla donde se concentran los puntos extraídos de las metodologías anteriores, las deficiencias encontradas y las propuestas nuevas para conformar la metodología y la realización de una investigación forense. *(Véase tabla 4.1)*

Tabla 4.1 Puntos extraídos, deficiencias encontradas y nuevas propuestas.

Puntos extraídos.	• **Propuesta de una fase de prevención (metodología de Kevin Mandia y Chris Prosise)** • **Propuesta de métodos en cada una de sus fases (metodología DFRW)** • **Un flujo definido porcada una de las etapas (metodología DOJ)**
Deficiencias encontradas.	• En su mayoría las metodologías no son generales. Evitando que puedan ser empleadas en cualquier dispositivo y tecnología encontrada en la escena del crimen. • En su mayoría no se proponen métodos para el manejo de grandes volúmenes de información. • En la mayoría de las metodologías no se proponen métodos para el análisis de datos oculta.
Puntos nuevos propuestos.	• Entrega de evidencia a la entidad una vez que el proceso ha terminado. • La eliminación segura de evidencia. • Propuesta de herramientas en cada una de sus fases. • La especificación de un objetivo por cada una de sus fases

2. Fases de la metodología propuesta.

Para poder organizar dentro de esta metodología, las actividades a realizar durante una investigación de cómputo forense que cumplan con los objetivos antes mencionados, se han dividido las tareas en ocho fases.

El conjunto de las ocho fases cumplen con los pasos generales que debe contener una metodología forense y responde a los retos que enfrenta el cómputo forense.

Al hacer la propuesta de cada una de las fases se tomó en cuenta el análisis realizado anteriormente, en donde se pudieron localizar las propuestas sobresalientes que se hacen en las metodologías que fueron analizadas, sus deficiencias y las nuevas propuestas.

Las fases o etapas que propone esta metodología son: fase de prevención, fase de identificación, fase de preparación, fase de adquisición de evidencia, fase de preservación, fase de análisis, fase de creación del reporte y fase de retroalimentación y devolución de evidencia.

En la siguiente tabla se muestran las fases que componen la metodología propuesta.*(Véase tabla 4.2).*

Tabla 4.2 Fases de la metodología propuestas y su equivalencia con las etapas generales de una investigación forense.

Fase de prevención.	Etapa propuesta.
Fase de identificación	Equivalente a la etapa de Identificación. –Etapas generales del cómputo forense-
Fase de preparación **Fase de adquisición de evidencia** **Fase de preservación**	Equivalente a la etapa de Preservación –Etapas generales del cómputo forense-
Fase de análisis	Equivalente a la etapa de Análisis -Etapas generales del cómputo forense-
Fase de creación del reporte	Equivalente a la etapas de Presentación -Etapas generales del cómputo forense-
Fase de retroalimentación y devolución de evidencia	Etapa propuesta.

En esta tabla se pueden observar sombreadas con color azul, las fases de la metodología propuesta que cumplen con las etapas generales que debe de tener

una metodología de cómputo forense y sombreadas con amarillo las etapas que fueron agregadas como parte de las nuevas propuestas que hace esta metodología.

La fase de prevención rescata el punto propuesto por la metodología de Kevin Mandia y Chris Prosise en la que propone una etapa de prevención.

Al implementar una fase de prevención dentro de la metodología forense se puede contar con acciones: la prevención de un posible incidente, la implementación de controles de seguridad y políticas, la preparación del equipo necesario para poder responder ante los posibles incidentes...

Esta fase mantiene al analista forense prevenido de los posibles incidentes que sufriera algún sistema. Este tipo de actividades podrán reflejar la mejoría, sobre todo si es una metodología que siga personal que se encuentre especializado en un sólo sistema. Es decir si es que esta metodología es aplicada en alguna entidad que cuente con un departamento dedicado a la investigación forense de sus sistemas.

Al prevenir los posibles incidentes de un sistema, se estará mejor preparado para enfrentar cualquier eventualidad.

La fase de identificación, la fase de preparación, la fase de adquisición de evidencia, la fase de preservación, la fase de análisis y la fase de creación del reporte cumplen con lo especificado en las etapas generales para la realización de una investigación forense.

En ellas se describen actividades para enfrentar los retos del cómputo forense como lo son el análisis de grandes volúmenes de información, o el análisis de información oculta. Además se proponen herramientas, técnicas y métodos para alcanzar el objetivo de cada una de las fases.

En cada una de estas fases de cuentan con actividades para mantener la integridad de la evidencia. Además de la propuesta de herramientas, técnicas y métodos

Mantener la integridad de la evidencia es un punto fundamental para que la evidencia sea aceptada en un procedimiento legal. Es por ello que en esta metodología se encontrará en cada fase, alguna actividad que cumpla este propósito.

Por último la *fase de retroalimentación y devolución de evidencia,* en esta fase se propone la retroalimentación de los resultados, compartiendo éstos con las demás áreas dedicadas a buscar la seguridad de los sistemas y con la alta gerencia. Realizar esta retroalimentación da la posibilidad de plantear propuestas para mejorar la seguridad del sistema, implementado políticas y controles de seguridad que prevengan la posibilidad de volver a tener un incidente del mismo tipo.

En esta fase también se implementan los puntos propuestos: la devolución de evidencia a la entidad y la eliminación segura de la evidencia.

Esta fase es implementada porque la información que se maneja, muchas veces trata de información confidencial o bien puede contener información de particulares.

Al realizar una investigación forense es importante que la entidad tenga la seguridad de que su información no será distribuida, o dada a conocer sin su autorización. De igual forma sirve como respaldo al analista forense para deslindarse de posibles fugas de información.

En resumen se busca que esta metodología cuente con:

- Acciones de prevención de incidentes.

- Que sea capaz de enfrentar los retos del cómputo forense –análisis de grandes volúmenes de información y análisis de información oculta-
- Que se tomen acciones para mantener la integridad de la evidencia.
- Que tome en cuenta la devolución de evidencia.
- Que incluya actividades para realizar la eliminación segura de información.

En la tabla 4.3 se muestran organizadas por fases, las aportaciones que se hacen para que la metodología cumpla con los puntos mencionados anteriormente.

Tabla 4.3 Origen de cada una de las fases que componen la metodología propuestas.

Fase de prevención.	Fase que rescata la aportación que se hace en la metodología Kevin Mandia y Chris Prosise de tener una etapa de prevención. -Acciones de prevención-
Fase de identificación	El establecimiento de la cadena de custodia ayuda a mantener la integridad de la evidencia.
Fase de preparación	Se incluye esta fase para cuidar la integridad de la evidencia.
Fase de adquisición de evidencia	Se propone el uso de técnicas para discriminar la información –problemas para el tratamiento de grandes volúmenes de información- Se cuida la integridad de la evidencia
Fase de preservación	Se proponen métodos y técnicas para mantener la integridad de la evidencia.
Fase de análisis	Se proponen técnicas para el análisis de grandes volúmenes de información. Se proponen métodos para el análisis de información oculta. Se cuida la integridad de la evidencia
Fase de creación del reporte	El conocimiento de los detalles del ataque brinca la posibilidad de prevenir futuros incidentes
Fase de retroalimen-tación y devolución de evidencia	Devolución de la evidencia Eliminación segura de la información.

3. Integración de las Fases de la Metodología Propuesta y Ubicación Dentro del Ciclo de Respuesta a Incidentes.

La metodología propuesta está conformada de ocho fases: Fase de prevención, fase de identificación, fase de preparación, fase de adquisición de evidencia, fase de preservación, fase de análisis, fase de creación del reporte y fase de retroalimentación y devolución de evidencia.

Al realizar una investigación forense se desarrolla cada una de las fases propuestas en esta metodología de manera consecutiva. En un flujo ideal se esperaría que se desarrollara una a una, cada fase hasta llegar al final y obtener el resultado final. Sin embargo es muy probable que durante el desarrollo de la investigación forense sea necesario regresar a cualquiera de las fases.

Por ejemplo se puede presentar el caso en el que durante el desarrollo de la fase de análisis se encuentre información que indique que la evidencia se encuentra almacenada en un dispositivo del cual no se realizó la adquisición de evidencia. En este caso será necesario regresar a la escena del crimen y realizar la adquisición de evidencia del dispositivo, para lo cual será necesario regresar a la fase de preparación, para después realizar la adquisición de evidencia y continuar con la metodología.

Aunque es posible realizar saltos hacia fases anteriores el regresar a fases para realizar adquisición de evidencia no es recomendable ya que entre más tiempo pase es más probable que la evidencia presente alteraciones. Por eso es importante realizar una buena fase de identificación para asegurarse de que la adquisición de evidencia se realizó por completo.

A continuación se esquematizan las fases que componen la metodología propuesta *(Véase fig. 4.1).*

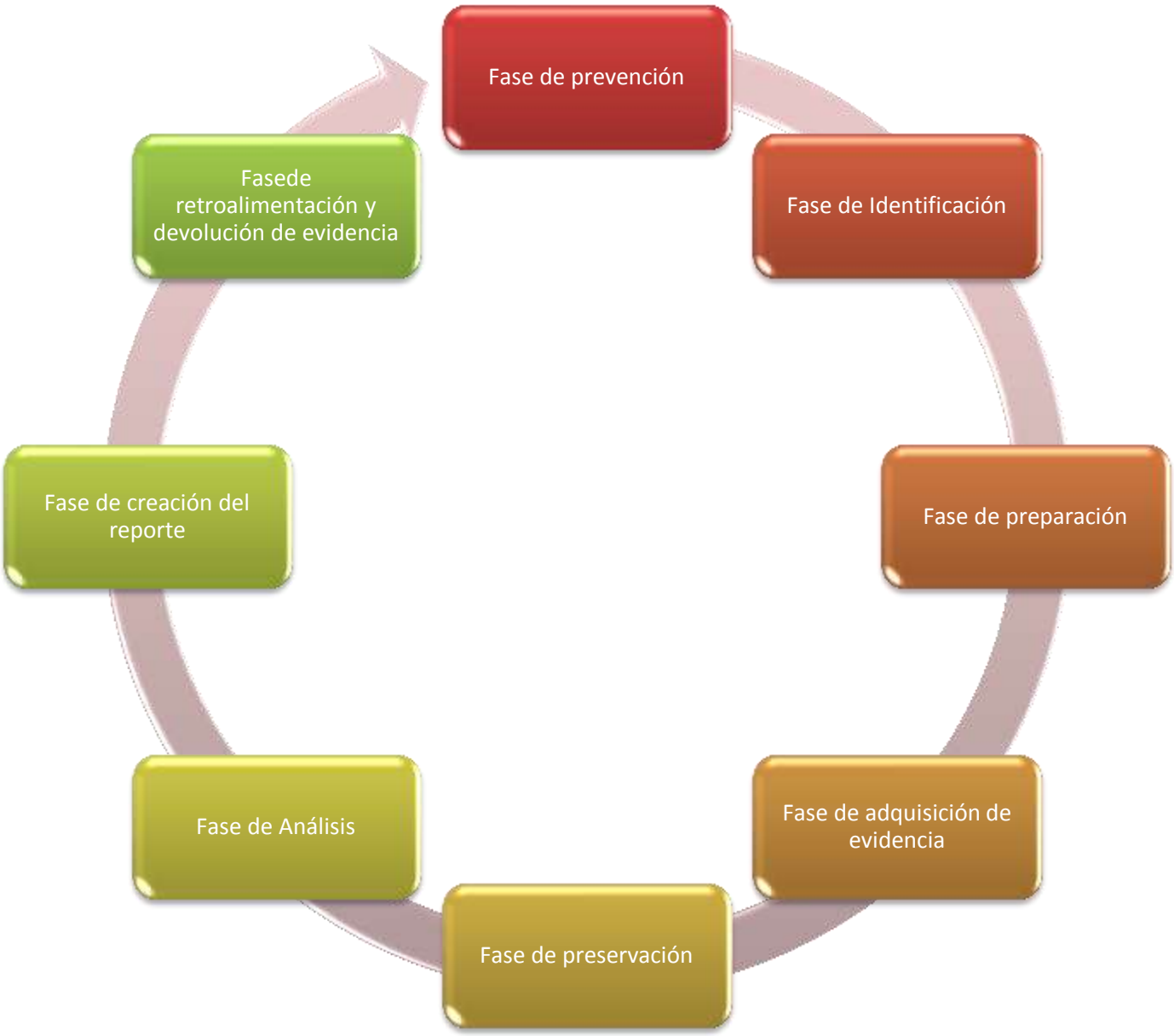


Figura 4.1 Fases que integran la metodología forense propuesta.

En esta figura se esquematizan las ocho fases que componen la metodología forense.

De las fases que se esquematizan en la figura 4.1 existen fases que pueden desarrollarse paralelamente a las demás como lo es la fase de creación del reporte, sin embargo hay otras que necesariamente deben de ir consecutivamente

para garantizar que la evidencia no se vea dañada y las pruebas que se presenten sean válidas ante una corte legal.

Existen tres grandes objetivos dentro de la metodología forense propuesta. El primero es lograr la adquisición de evidencia, el segundo la realización del análisis y por último la presentación de resultados.

Para cada uno de estos objetivos se plantean fases que ayuden a su cumplimiento. Para lograr el primer objetivo –lograr la adquisición de evidencia- se proponen 3 fases: la fase de identificación, la fase de preparación y por último la fase de adquisición de evidencia *(Véase fig. 4.2)*.

Figura 4.2 Fases para lograr la adquisición de evidencia.

Dentro de la fase de identificación se hará el reconocimiento de todos los lugares en donde se pueda encontrar evidencia que ayude al caso. Una vez identificados se pasará a la etapa de preparación en donde se analizarán las características de cada uno de los dispositivos contenedores de evidencia para

preparar el equipo necesario tanto de hardware como de software que ayudará a realizar la adquisición de evidencia.

Una vez preparado el equipo entonces se puede pasar a la fase de adquisición de evidencia donde se podrán recuperar aquellos datos que sirvan para resolver el caso.

Como segundo objetivo se tiene la realización del análisis. Para poder cumplir este objetivo es necesario contar con toda la evidencia del caso por eso es importante realizar una muy buena adquisición de evidencia.

Para realizar el análisis se proponen tres fases en esta metodología: La adquisición de evidencia, la preservación y el análisis *(Véase fig. 4.3)*.

Figura 4.3 Fases para realizar el análisis.

Al realizar la fase de adquisición de evidencia obtendremos todo el material que será sometido a análisis. Todo este material tendrá que ser trasladado en el laboratorio forense con el equipo adecuado, es necesario garantizar que durante el traslado no sufrirá ningún tipo de alteración, es decir, que la evidencia se

encuentre integra. Esto se realizará en la fase de preservación.

Una vez que se tiene la garantía de que la evidencia es auténtica entonces es confiable realizar el análisis, actividad que se realizará en la fase de análisis, aplicando diferentes métodos.

Por último se tiene el objetivo de la presentación de evidencia. Para lograr este objetivo se proponen en esta fase tres fases: análisis, creación del reporte y retroalimentación y devolución de evidencia *(Véase fig. 4.4)*.

Figura 4.4 Fases para la presentación de la evidencia.

Al realizar el análisis de la evidencia se obtendrán los resultados los cuales se presentarán en el reporte junto con los procedimientos que se siguieron para identificar la evidencia, adquirirla, transportarla y mantener su integridad.

En la fase de retroalimentación y devolución de evidencia se realizarán las propuestas para mejorar el sistema evitando tener incidentes del mismo tipo y se hará la devolución de evidencia a la entidad que la haya proveído.

Todas las fases de la metodología se encuentran relacionadas para cumplir diferentes objetivos particulares, al ir cumpliendo estos objetivos se logra la realización de una investigación forense exitosa *(Véase fig. 4.5).*

Figura 4.5 Relación de las fases de la metodología forense.

En la fig. 4.5, se puede ver como se encuentran relacionadas todas las fases de la metodología forense para cumplir los tres objetivos de la metodología –adquisición, realización y presentación de la evidencia-.

Dentro de este esquema no se encuentra la fase de prevención ya que es una fase que se realiza antes y después de que se atiende un incidente de seguridad.

En la fase de prevención se toman las medidas necesarias para poder enfrentar algún incidente en donde se tenga que realizar una investigación de cómputo forense, se prepara el equipo –hardware y software- que pueda ser requerido en el momento de dar respuesta al incidente. Se analizan las amenazas a las que esté sometido el sistema, se detectan los lugares sensibles y los nuevos tipos de ataques.

Se vuelve a entrar en la etapa de prevención una vez que se ha terminado de realizar la investigación forense. Ya con los resultados de la información se puede prever un incidente del mismo tipo.

3.1 Ubicación de la metodología dentro del ciclo de respuesta a incidentes.

Ya que se conocen cuáles son las fases que componen a la metodología de cómputo forense es necesario saber cuál es el momento en el que ésta debe de ser ejecutada.

Para saber en qué momento se iniciará la investigación de cómputo forense es necesaria ubicar la metodología propuesta dentro del ciclo de respuesta a incidentes de algún sistema. A continuación se muestra una imagen con del ciclo de respuesta al incidente que se desempeña por parte del equipo de cómputo forense *(Véase fig. 4.6).*

Figura 4.6 Ciclo de respuesta a incidentes por parte del equipo de cómputo forense.

En este ciclo se pueden observar las etapas de: monitoreo del sistema, detección de incidentes, respuesta a incidentes y aplicación de la metodología forense propuesta y la creación de sistemas e implementación de controles de seguridad y políticas.

Se puede notar que la aplicación de la metodología forense se encuentra justo después de la detección del incidente, es importante mencionar que una vez que se ha detectado el incidente el primer grupo que entra en acción es el grupo de respuesta a incidentes y posteriormente entrara el equipo de cómputo forense.

La razón de este orden es porque muchas veces se tiene que priorizar la recuperación del servicio (si es que este se ha dañado), aunque las acciones que se tengan que tomar dañen la evidencia que se pueda encontrar.

Una vez que se ha recuperado el sistema entonces se realizará la recuperación evidencia para hacer el análisis pertinente que muestre los detalles del incidente.

Muchas veces el trabajo que tienen que realizar ambos equipos se puede coordinar para lograr los mejores resultados. Al coordinarse pueden lograr que la recuperación del sistema sea pronta y con la menor cantidad de evidencia pérdida.

Al final ambos equipos llegan a resultados que sirven para un mismo fin, el de mejorar la seguridad del sistema para evitar incidentes del mismo tipo. Es por eso que en esta metodología propuesta se presenta una fase llamada “fase de retroalimentación” en la cual se sugiere que una vez que se cuenta con todos los detalles del incidente, se compartan los resultados con las demás áreas de seguridad y la alta gerencia, para que se puedan implementar políticas y controles de seguridad que eviten que el sistema vuelva a presentar incidentes del mismo tipo que puedan ocasionar daños y pérdidas

A continuación se describirán cada una de las fases que componen la metodología forense propuesta en este capítulo.

4. Descripción de las Fases de la Metodología Propuesta.

Ya se ha especificado cuales son las fases que componen la metodología forense y de forma somera se ha mencionado que actividades se realizarán en cada fases.

A continuación se hará una descripción precisa de cada una de las fases: fase de prevención, fase de identificación, fase de preparación, fase de adquisición de evidencia, fase de preservación, fase de análisis, fase de creación del reporte y fase de retroalimentación y devolución de evidencia.

En esta descripción se especificarán cuáles son los objetivos de cada fase, cuáles son las preguntas claves que se deben de realizar, y los pasos para conseguir el objetivo.

Posteriormente se desarrollará cada uno de los pasos propuestos para cada fase, especificando cuáles son las actividades que se tienen que realizar en dicho paso. Al finalizar la descripción de todos los pasos de la fase se presenta un listado con los métodos y herramientas que se pueden utilizar, para facilitar las actividades a realizar.

Al final de cada una de las fases se presenta una tabla que contiene en forma de resumen el objetivo de la fase, las preguntas clave, los pasos a realizar y los métodos y herramientas propuestas.

4.1 Fase de Prevención.

Esta fase tiene como objetivo tener el conocimiento de los sistemas a los que se les va a atender y contar con el equipo suficiente para atenderlos.

Para lograr este objetivo se realizan actividades que ayudan a formar un panorama del tipo de escenarios que se pueden encontrar *(Véase fig.4.7)*.

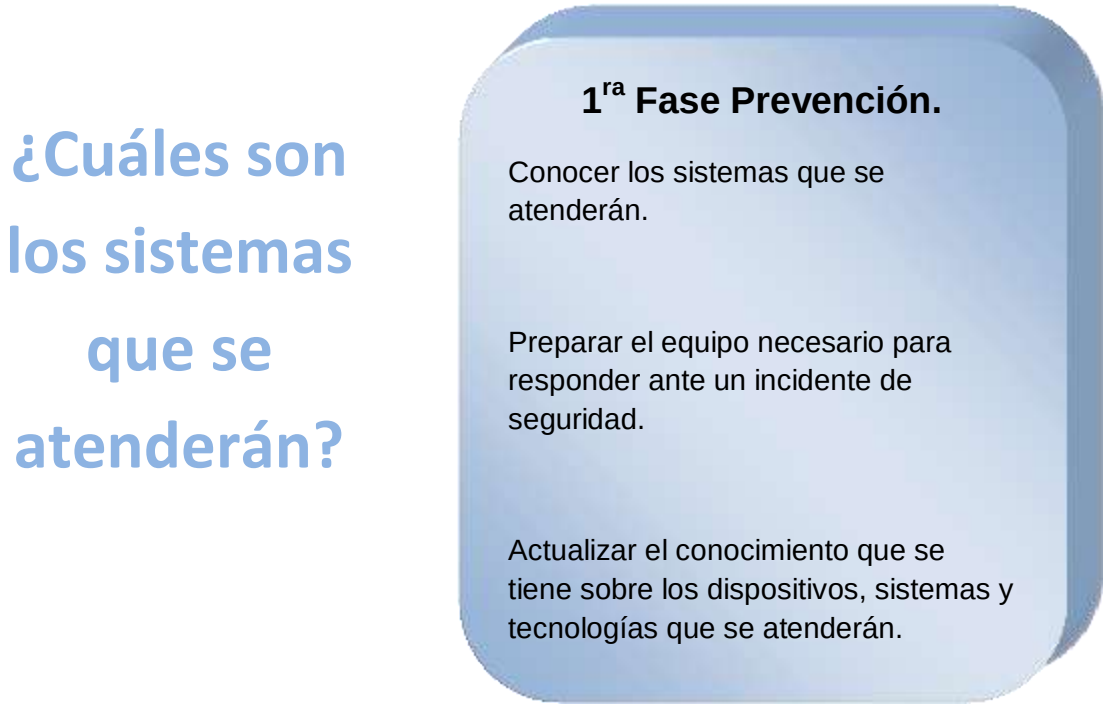


Figura 4.7 Fase de prevención.

1. Conocer los sistemas que se atenderán.

   Para poder reaccionar ante los incidentes de seguridad que se presenten hay que mantenerse actualizado ante el nuevo tipo de tecnologías que se utilizan, los nuevos dispositivos, sistemas operativos que usan y las redes de comunicación. Así como las vulnerabilidades que cada uno presenta y las amenazas a las que se encuentra expuesto.

   De ser que el campo que se vaya a atender, este acotado, por ejemplo, que sólo se atiendan los incidentes ocurridos dentro de determinada empresa, entonces en esta fase se hará el análisis del sistema, la infraestructura utilizada para operar, el tipo de información que se maneja, la forma en la que viajan los datos –cifrada, en claro, comprimida, con permisos-, el tipo de usuarios

con los que consta el sistema, el tipo de permisos que tiene cada uno, etc.

Tener presente este tipo de información prevendrá al analista sobre el equipo y el conocimiento que deberá poseer para reaccionar de la mejor manera ante cualquier incidente. Podrá prever la capacidad de almacenamiento que necesitará para recuperar evidencia, el tipo de conexiones de alimentación con las que debe contar, así como identificar cuáles son los lugares que le pueden proporcionar más información dependiendo del incidente ocurrido.

Contando con toda la información acerca de los sistemas y su infraestructura es posible realizar manuales de cómo responder ante un incidente tanto para los integrantes del equipo de cómputo forense como para los usuarios.

En resumen poseer toda esta información asegura que la respuesta al incidente sea más rápida y asertiva.

2. Preparar el equipo necesario para responder ante un incidente de seguridad.

   Es necesario que se prevenga el analista forense, con equipo tanto de hardware como de software, para dar respuesta a los incidentes que se puedan presentar.

   Para que el analista forense pueda prevenir el equipo que utilizará, es necesario que conozca los sistemas que atenderá y que este actualizado en cuanto a la nueva tecnología. Es común que cuando cambia la tecnología con ella cambie el tipo de conexiones que se utilizaban.

Dentro del equipo de hardware que se tiene que prever se encuentran: los cables necesarios para conectar cualquier dispositivo de almacenamiento y el equipo de almacenamiento suficiente para guardar la evidencia encontrada. En caso de necesitar hacer la extracción de datos, estos dos elementos serán parte fundamental del equipo, para dar respuesta ante un incidente.

3. Actualizar el conocimiento que se tiene sobre los dispositivos, sistemas y tecnologías que se atenderán.

   Es importante que, una vez que se tenga el conocimiento de cuáles son las características del ó de los sistemas que se van a atender, se actualicé el analista forense, sobre las vulnerabilidades, los nuevos ataques que puedan dañar el sistema y el tipo de software que le ayude a dar respuesta al incidente etc.

Herramientas:

Las herramientas que se pueden utilizar en esta fase son:

- Toda fuente de información confiable sobre vulnerabilidades, malware y nuevas tecnologías.
- Información sobre algoritmos de cifrado.
- Técnicas para ocultar información.
- Mapas de la infraestructura.
- Manuales del sistema.
- Programas de respuesta a incidentes.
- Descripción del funcionamiento del sistema.
- Organización jerárquica de los usuarios.
- Información de la entidad y del sistema.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de prevención y como fue cubierta cada etapa *(Véase tabla 4.4)*.

Tabla 4.4 Preguntas clave, etapas y herramientas de la fase de prevención.

Fase de Prevención	
Preguntas claves	• ¿Cuáles son los sistemas que se atenderán?
Etapas	• Conocer los sistemas que se atenderán • Preparar el quipo necesario para responder ante un incidente de seguridad • Actualizar el conocimiento que se tiene sobre los dispositivos, sistemas y tecnologías que se atenderán
Herramientas	• Fuentes de información confiable sobre vulnerabilidades, malware y nuevas tecnologías. • Programas de respuesta a incidentes. • Descripción del funcionamiento del sistema. • Equipo de hardware y software según los requerimientos de los sistemas que se vayan a atender.

4.2 Fase de Identificación.

Esta fase tiene como objetivo establecer el plan de acción para la recuperación de evidencia con base en la información que se tenga del incidente y del sistema afectado.

Para lograr este objetivo se realizan actividades que ayuden a conocer el tipo de incidente que tuvo lugar y cuáles son las partes involucradas *(Véase fig.4.8)*.

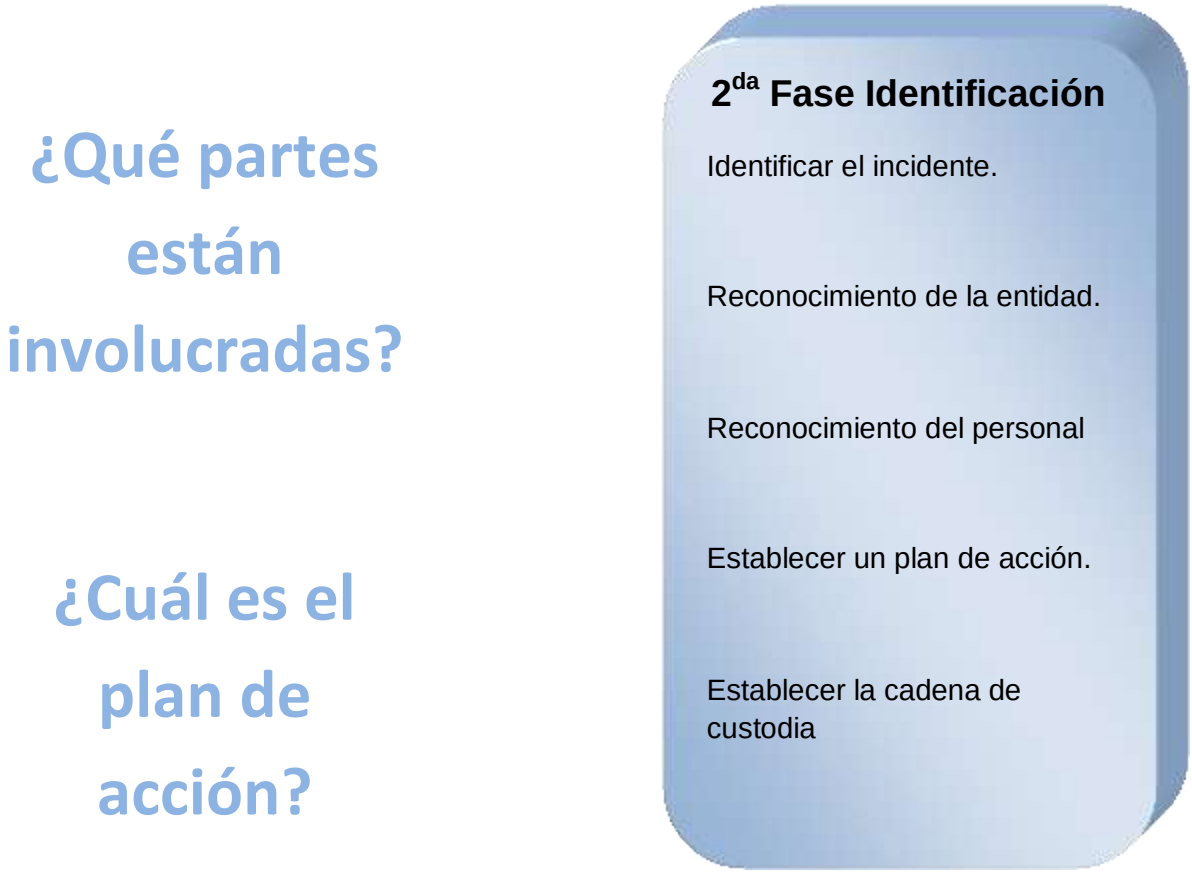


Figura 4.8 Fase de identificación.

1. *Identificar el incidente*. Una vez que se ha reportado el incidente se debe conocer como fue detectado qué o quiénes emitieron la alarma y cuál fue la razón por la cual se activó la alarma.

   Con este tipo de información se deberá deducir que tipo de incidente es –acceso no autorizado, código malicioso, denegación de servicio, escaneos, mal uso de los recursos de internet-. Una vez que se ha identificado el incidente se tendrá una clara idea de cuáles son las partes en donde se tendrá que hacer la búsqueda de evidencia.

   Los primeros datos que se podrán tener del incidente son:

- Día y hora en el que fue reportado.
- Responsable del reporte del incidente.
- Evento que activó la alarma.

2. *Reconocimiento de la entidad.* Continuando con la fase de identificación se debe conocer al menos de manera general la forma en la que opera la entidad dañada –cómo viajan sus datos, la configuración de sus equipos, el tipo de usuarios que tiene, cómo viaja su información, sus políticas, etc.

    - *Organización de la entidad*. Conocer la forma en la que almacenan, comparten y distribuyen su información es importante ya que se podrán localizar los posibles lugares que contengan evidencia dependiendo del incidente reportado.

    - *Las políticas de la entidad.* Es necesario conocer las políticas de seguridad de la empresa para saber en que momento se puede llevar a cabo el plan de acción, no se puede hacer caso omiso de estas políticas ya que son los procedimientos que tiene la entidad establecidos para poder tener los mejores resultados, de no seguirlos podríamos causar desorden y pérdida de tiempo estropeando el trabajo de los demás.

      Es importante que se obtenga el permiso de la persona responsable para actuar sobre el sistema ya que de lo contrario se podría caer en alguna falta al recabar información clasificada.

    - *La estructura de red de ser necesario.* Si en el incidente ocurrido se vio involucrada la red entonces será necesario hacer un análisis de ella por lo cual se tendrá que tomar en cuenta la red como un elemento más de donde habrá que recabarse evidencia.

      Antes de hacer la recolección de evidencia de la red se deberá

conocer la estructura de red, con lo cual se logrará acotar los espacios en los que haya evidencia y no perder tiempo ni recursos recopilando datos de toda la red que al final no proporcionarán la información necesaria.

Al conocer la entidad y su organización podremos obtener datos como:

- Hardware y software involucrado.
- Lugares clave para la recolección de evidencia.
- Momentos en los que se podrá emplear el plan de acción.

3. *Reconocimiento del personal.* Una de las fuentes de las cuales se obtendrá valiosa información será del personal que tiene contacto constante con los sistemas, de las personas que detectaron el incidente, y las personas que se vean involucradas.

Al conocer al personal de la entidad se puede obtener información como:

- Quién o qué reporto el incidente.
- Cuál es el personal involucrado.
- La naturaleza del incidente.
- Cuándo ocurrió el incidente.
- Quién suele tener contacto con esos sistemas.
- Cuál es el comportamiento normal del personal.

4. *Establecer un plan de acción.* Con toda la información recabada en la los tres puntos anteriores –el incidente, la entidad y el personal- es posible deducir cuales son los lugares en donde se pueden encontrar datos que sirvan como evidencia para reconstruir los hechos y saber qué fue lo que paso.

   Los lugares en donde se pueden encontrar los datos que le sirvan al analista forense para reconstruir los hechos, pueden estar almacenados en

cualquier dispositivo que almacene de forma digital los datos. Una vez que se cuente con el listado de los dispositivos que tendrán que ser atendidos para extraer de ellos la evidencia, se debe establecer el orden en el que se hará la extracción.

Para establecer el orden en el que se atenderán los diferentes dispositivos, se tomará en cuenta la volatilidad que tienen los datos en cada uno de los dispositivos. De esta manera se asegura conseguir la mayor cantidad de evidencia.

5. *Establecer la cadena de custodia.* El establecimiento de la cadena de custodia es un aspecto primordial pues de esto depende que la evidencia sea confiable y pueda presentarse en un procedimiento legal.

   La cadena de custodia se establecerá desde el primer momento en el que se entra en contacto con la evidencia y con los componentes que la contienen.

   Para establecer la cadena de custodia es necesario:

   - Que se describa detalladamente la forma, el estado y el lugar donde se encontró la evidencia.
   - Que se compruebe que no se vio alterada la evidencia. Es decir que se conserva integra desde el momento en el que se encontró hasta el momento en el que se presenta ante una corte penal.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de esta fase son:

Reconocimiento del incidente.

- Reportes de la detección de la intrusión y las bitácoras basadas en la red para identificar el incidente.
- Elaboración de lista de palabras clave.

Reconocimiento de la entidad.

- Planos de la distribución de equipos en la entidad.
- Topología de la red.
- Elaboración de lista de palabras clave.

Reconocimiento del Personal.

- Diagrama jerárquico del personal y las actividades que realiza dentro de la entidad.
- Entrevistas de los administradores de sistema que pudieran haberse percatado de algunos detalles técnicos del incidente.
- Entrevistas del personal de gerencia quienes pudieran haberse percatado de algunos eventos en el negocio que pueda proveer contexto al incidente.
- Cuestionarios contestados por el personal involucrado.
- Elaboración de lista de palabras clave.

Establecer un plan de acción.

- Orden de volatilidad de los datos.

Cadena de custodia.

- Fotos y video de la escena del crimen.
- Herramientas para implementar funciones hash a las imágenes obtenidas.
- Formatos para establecer la cadena de custodia.

Hacer una correcta valoración de los equipos será vital para obtener una investigación exitosa. El análisis será sólo de los datos extraídos, y aunque es posible hacer una segunda recuperación de datos lo más probable es que los datos se encuentren modificados o eliminados.

La duración de esta fase debe ser lo más corta posible, entre menos tiempo lleve localizar los lugares clave para encontrar la evidencia será mejor. Se debe tener en cuenta que cada segundo que pasa puede alterar de manera significativa la evidencia.

Toda la información recolectada durante esta fase será de gran utilidad durante la fase de análisis. Por tal razón es recomendable que se tome nota de todos los detalles observados, dados por el personal o indagado a partir de las entrevistas y cuestionarios.

Se recomienda contar con una libreta a la mano donde se anoten todas aquellas palabras clave que después tengamos que recodar o nos sirvan para analizar la información.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de identificación y como fue cubierta cada etapa *(Véase tabla 4.5)*.

Tabla 4.5 Preguntas clave, etapas y herramientas de la fase de identificación.

Fase de Identificación	
Preguntas claves	• ¿Qué partes están involucradas? • ¿Cuál es el plan de acción?
Etapas	• Identificar el incidente. • Reconocimiento de la entidad. • Reconocimiento del personal. • Establecer un plan de acción. • Establecer la cadena de custodia.
Herramientas	• Reportes de la detección del incidente • Bitácoras • Planos de la distribución de equipos • Topología de la red • Diagramas jerárquicos del personal • Entrevistas y cuestionarios • Orden de volatilidad de datos • Fotos y videos de la escena del crimen • Herramientas para implementar funciones Hash • Formatos de cadena de custodia • Elaboración de lista de palabras clave.

4.3 Fase de Preparación.

Esta fase tiene como objetivo identificar el equipo de hardware y software que se necesitará para realizar la recuperación de la evidencia.

Para lograr este objetivo se realizan actividades que ayuden a conocer las características de hardware y software de los equipos involucrado en el incidente y

conocer exactamente el equipo que se necesita para realizar la recuperación *(Véase fig.4.9)*.

¿Qué se necesita para hacer la adquisición?

Figura 4.9 Fase de Preparación.

Para cuando se haya llegado a esta fase se tendrá pleno conocimiento del o de los dispositivos que contiene la evidencia. Para poder preservarlo primero tenemos que conocer las características del equipo que se empleará para la recuperación.

1. *Identificación del equipo.* Se recabarán todas las especificaciones técnicas del dispositivo contenedor de evidencia como por ejemplo:
    - El tipo de puertos que tiene.
    - La capacidad de almacenamiento que posee.

- El espacio que ocupa la evidencia.
- Tipo de configuración que tiene.
- Tipo de conexiones que posee en ese momento.
- Lugar en donde se encuentra.
- Si se requiere que este encendido o puede apagarse.

Dependiendo de estos datos será que se seleccione el tipo de equipo requerido para poder hacer la recuperación de la evidencia. Es importante contar con discos de gran capacidad para poder hacer la recuperación de toda la evidencia necesaria, hay que tomar en cuenta que la tecnología se desarrolla rápidamente y el espacio de almacenamiento cada vez es mayor.

2. *Identificación del equipo software.* Se tendrá que identificar el tipo de software que utiliza el equipo que contiene la evidencia pues de ello dependerá el tipo de herramientas que se utilicen para la preservación.

3. *Preparación del equipo.* Una vez que ya se identificaron las características que debe de tener el equipo en el cual se almacenará la evidencia para su posterior análisis, se debe de realizar la configuración correcta del equipo.

   Se debe de cuidar que la configuración favorezca la integridad de la evidencia. Para lo cual se debe tomar en cuenta:

- El equipo de almacenamiento se encuentre limpio[21].
- El formato de almacenamiento que se usará sea el adecuado.
- Que el equipo cuente con mecanismos de protección contra escritura que se puedan aplicar una vez almacenada la evidencia.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de esta fase son:

- Herramientas de software apropiadas – herramientas de software aprobadas- para el sistema que se desea atender.
- Herramientas de hardware apropiadas – herramientas de hardware aprobadas- para el sistema que se desea atender.
- Equipo de almacenamiento de gran capacidad.
- Herramientas de software o hardware que garanticen la integridad de la evidencia.
- Unidad de cómputo forense.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de preparación y como fue cubierta cada etapa *(Véase tabla 4.6)*.

[21] Por limpio se debe entender que es un dispositivo que no ha contenido información anteriormente. Los sectores del disco no contienen información.

Tabla 4.6 Preguntas clave, etapas y herramientas de la fase de preparación.

Fase de Preparación	
Preguntas claves	• ¿Qué tipo de técnica se usara? • ¿Qué se necesita?
Etapas	• Identificación del equipo hardware. • Identificación del equipo software. • Preparación del quipo.
Herramientas	• Herramientas de software apropiadas –herramientas de software aprobadas- para el sistema que se desea atender. • Herramientas de hardware apropiadas –herramientas de hardware aprobadas- para el sistema que se desea atender. • Equipo de almacenamiento de gran capacidad. • Herramientas de software o hardware que garanticen la integridad de la evidencia. • Unidad de cómputo forense

4.4 Fase de Adquisición de Evidencia.

Esta fase tiene como objetivo realizar la adquisición de la evidencia digital encontrada en la escena del crimen.

Para lograr este objetivo se realizan actividades que ayuden a recuperar la evidencia de la escena del crimen *(Véase fig. 4.10)*.

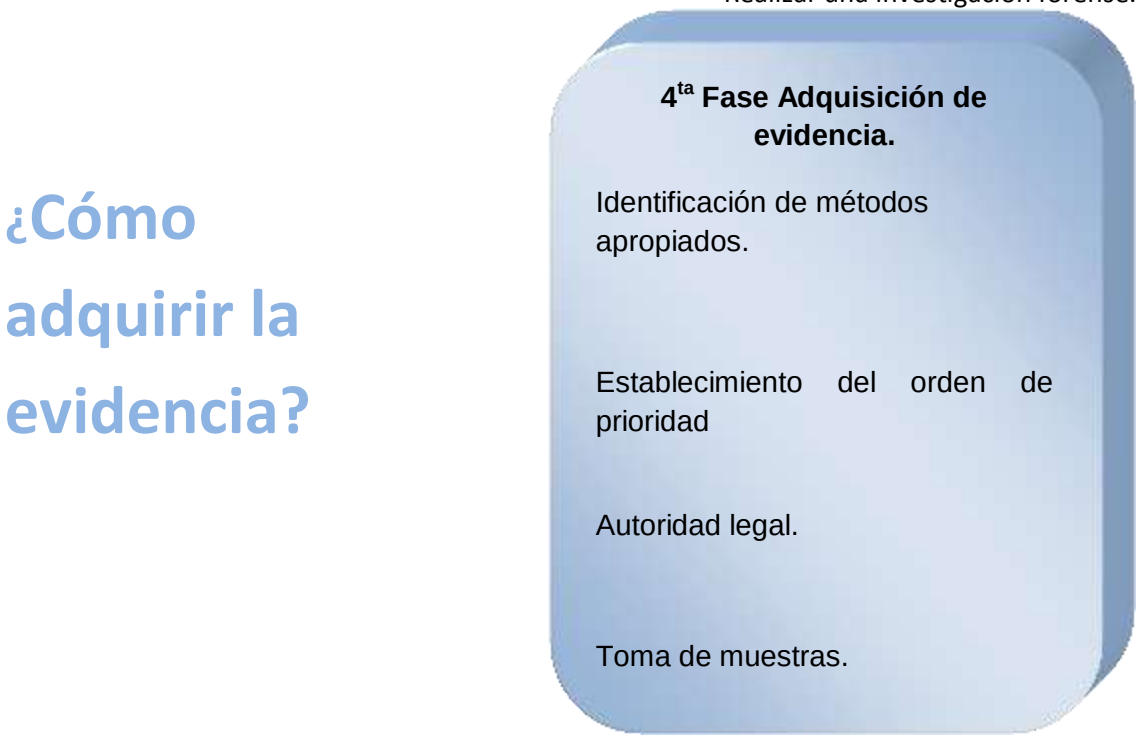


Figura 4.10 Fase de adquisición de evidencia.

1. *Identificación de métodos apropiados.* En esta fase se analizará cuales son los métodos apropiados para la adquisición de evidencia. Puede ser que la capacidad de los equipos que contienen la evidencia sobrepasa la posibilidad de realizar una imagen forense que sea útil para el análisis, para lo cual existen otro tipo de métodos que pueden servir.

   Como por ejemplo la toma de muestras, es decir, sólo parte del contenido del dispositivo que almacene la información que se necesita.

   O puede ser que los dispositivos tengan que ser trasladados al laboratorio forense donde se tendrán que analizar, para este caso, se debe de contar con mecanismos y equipo que permita el traslado.

2. *Autoridad legal.* Siempre debe de contarse con el permiso de la autoridad legal para hacer la adquisición de evidencia, de lo contrario

podría el analista estar cometiendo un delito por la obtención de información sin autorización.

3. *Toma de muestra.* Cuando se hace la adquisición de la evidencia se debe de comprobar que esta es integra, es decir que no ha sufrido ningún tipo de alteración y que corresponde unívocamente a los datos ubicados en el dispositivo que los contenía originalmente.

4. *Reporte.* Todos los pasos realizados en esta etapa deberán de ser justificados y reportados tanto el procedimiento como las herramientas y equipo utilizado.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de esta fase son:

- Buenas prácticas para la adquisición de evidencia.
- Aprobación legal para la adquisición de evidencia.
- Software y hardware aprobado.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de adquisición de evidencia y como fue cubierta cada etapa *(Véase tabla 4.4)*.

Tabla 4.7 Preguntas clave, etapas y herramientas de la fase de adquisición de evidencia.

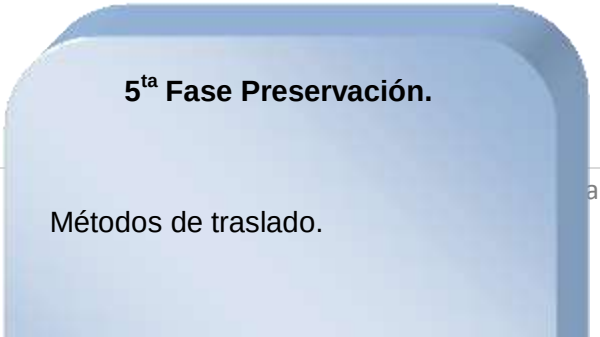
Fase de Adquisición de evidencia

Preguntas claves	• ¿Cómo adquirir la evidencia?
Etapas	• Identificación de métodos apropiados • Establecimiento del orden de prioridad • Autoridad legal • Toma de muestras
Herramientas	• Buenas prácticas para la adquisición de evidencia. • Aprobación legal para la adquisición de evidencia. • Software y hardware aprobados • Métodos de adquisición de evidencia de grandes volúmenes de información –toma de muestras-

4.5 Fase de Preservación.

Esta fase tiene como objetivo mantener integra la evidencia, así como el seguimiento de la cadena de custodia durante el traslado de la escena del crimen al laboratorio forense.

Para lograr este objetivo se realizan actividades que ayudan a garantizar la integridad de la evidencia *(Véase fig. 4.11)*.



¿Cómo conservar la evidencia?

Figura 4.11. Fase de preservación.

1. *Métodos de traslado.* Una vez que se ha realizado la adquisición de la evidencia es necesario tomar en cuenta aspectos que pudieran dañar la evidencia durante el traslado.

   Por ejemplo al almacenar la evidencia en discos duros estos podrían verse alterados al presentarse ante campos magnéticos, por lo cual es recomendable protegerlos guardándolos en bolsas de Faraday.

   En el caso de que sea imposible adquirir la evidencia por el estado en el que se encuentra el dispositivo o la evidencia, se deberá pedir la salida de este dispositivo para ser llevado al laboratorio forense, en donde se cuenta con material y condiciones controladas que permiten la adquisición de la evidencia.

   Para poder trasladar el dispositivo que se encontró en la escena del crimen se debe tomar medidas de precaución ya que al trasladar la fuente original de la evidencia, sin antes haber hecho la imagen o la adquisición de evidencia, se está trasladando la única fuente de donde se pueden obtener los datos que servirán como evidencia y la pérdida de datos o del dispositivo durante el traslado seria irreparable.

Lo más recomendable es tratar de no alterar su estado y mantenerlo fuera de cualquier variable que pudiera alterar la evidencia.

2. *Seguimiento de la cadena de custodia.* Ya sea, que lo que se traslade sea el dispositivo contenedor de la evidencia, o la imagen de la evidencia extraída de él/los dispositivos, la cadena de custodia tendrá que mantenerse.

   Para mantener la cadena de custodia debe especificarse siempre un responsable que registre, la hora en la que recibe la evidencia, la hora en la que la deja, en qué estado la recibe y en qué estado la deja. Así como las actividades que realiza con ella, comprobando que las actividades practicadas no han alterado la evidencia.

   Al dejar la evidencia en manos de otra persona tiene que registrar a esta persona como el nuevo responsable.

   Cuando la evidencia es adquirida debe de ser inmediatamente etiquetada y descrita estableciendo así la cadena de custodia.

   Al transportar la evidencia esta debe de ser empaquetada y marcada de tal manera que se garantice que durante el traslado no se verá alterada.

   Respaldos. Una vez que se ha adquirido la evidencia, es necesario manejar una política de respaldos en donde se establezca el número de copias que se deberán hacer de cada una de las adquisiciones obtenidas para el análisis.

   El contar con respaldos evita que se pierda la evidencia por algún desconocido o acción intencional. Una de las copias de la adquisición de la evidencia se recomienda que se quede guardada en un sitio seguro y de acceso restringido, esta copia servirá como repuesto previniendo que

las otras copias pudieran sufrir algún daño o pérdida durante el proceso de análisis.

Dependiendo del número de analistas que trabajen sobre la evidencia y de cómo se organicen en tiempos, y la evidencia que vayan a examinar, será el número de duplicados que habrán de tenerse.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de esta fase son:

- Bolsas de Faraday – para mantener los equipos exentos de daño producido por campos magnéticos o en el caso de celulares permita además que no se vea alterada la evidencia por la entrada de mensajes llamadas o actualizaciones-
- Formatos bien establecidos para conservar la cadena de custodia.
- Políticas de respaldos.
- Lugares seguros de almacenamiento.
- Herramientas de software y hardware que garanticen la integridad.
- Etiquetado de evidencia. Para etiquetar la evidencia se suele manejar etiquetas, sellos, parches o firmas que no puedan ser falsificables.

  Al contar con etiquetas no falsificable el analista notará fácilmente si el paquete donde se encuentra la evidencia fue violado. Un método que se utiliza para contar con una etiqueta no falsificable

es utilizar una firma autógrafa encime de un sello o etiqueta.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de preservación y como fue cubierta cada etapa *(Véase tabla 4.8)*.

Tabla 4.8 Preguntas clave, etapas y herramientas de la fase de preservación.

Fase de Preservación	
Preguntas claves	• ¿Cómo conservar la evidencia?
Etapas	• Métodos de traslado • Seguimiento de la cadena de custodia. • Respaldos
Herramientas	• Bolsas de Faraday • Formatos para conservar la cadena de custodia • Políticas de respaldo • Lugares seguros de almacenamiento • Herramientas de hardware y software que garanticen la integridad. • Etiquetas

4.6 Fase de Análisis.

Esta fase tiene como objetivo encontrar los datos que puedan servir para refutar o comprobar una hipótesis, correlacionar estos datos entre sí y con la información obtenida previamente, dando así respuesta a las preguntas de ¿Qué fue lo que sucedió?, ¿Cómo sucedió? ¿Quién lo hizo?…

Para lograr este objetivo se realizan actividades de búsqueda de evidencia dentro de las imágenes previamente capturadas *(Véase fig. 4.12)*.

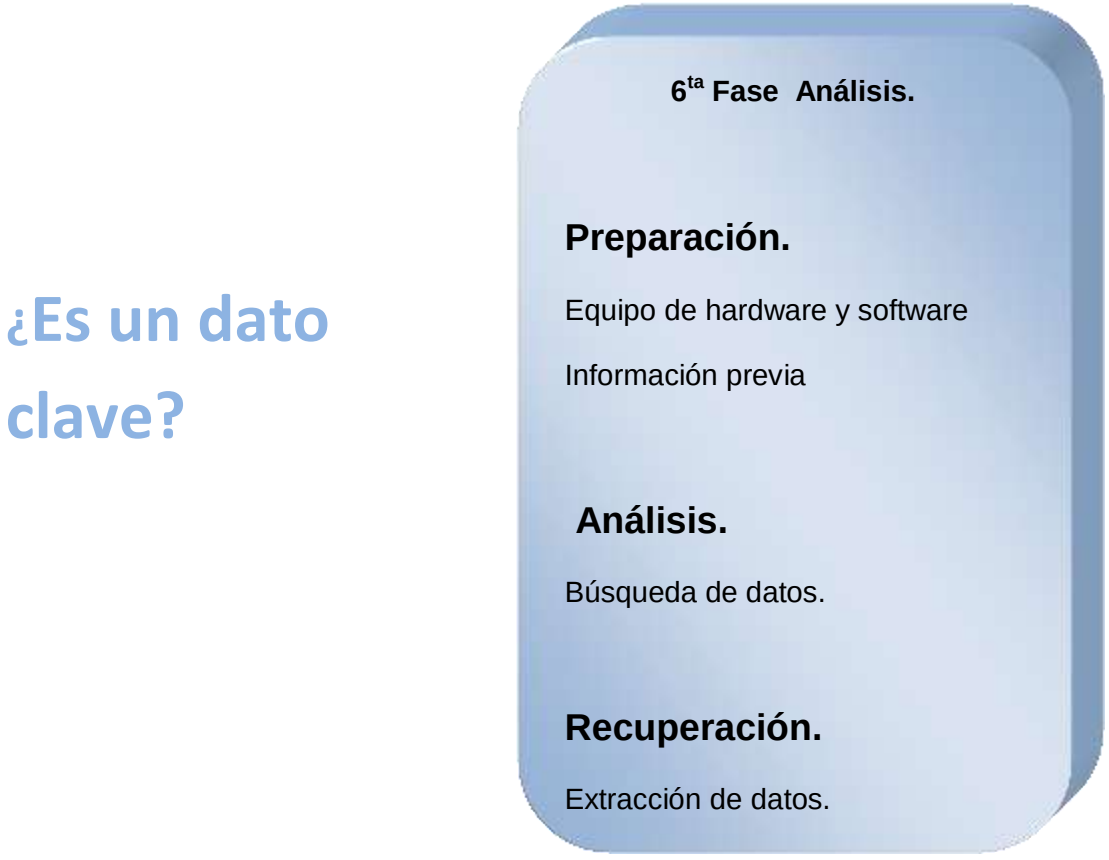


Figura 4.12 Fase de Análisis.

1. *Preparación.* Para poder comenzar con el análisis de la evidencia capturada en la escena del crimen, es necesario contar con equipo de software y hardware previamente instalado, configurado y probado. La elección de qué sistema operativo, herramientas de software o incluso hardware dependerán del tipo de evidencia que se desee analizar y del dispositivo en donde se tenga almacenada.

Dentro de las cosas que hay que tener a la mano para realizar el análisis de la evidencia es la lista de las palabras claves que se han recabado durante la investigación así como información obtenida de las fases previas.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de preparación para el análisis son:

- Equipo de software y hardware para realizar el análisis.
- Equipo para preservar la evidencia integra.
- Laboratorio forense.
- Lista de palabras clave.

2. *Análisis.* El objetivo del análisis es obtener los datos que ayuden a comprobar o refutar alguna hipótesis o bien a crear una nueva hipótesis. Los métodos y técnicas que se apliquen en esta fase variaran dependiendo del tipo de información que se desea buscar, el lugar donde se encuentra almacenada y el tamaño de la evidencia capturada.

   Por ejemplo será diferente el procedimiento para buscar información acerca de una imagen que la búsqueda de información dentro de una bitácora.

   Una de las técnicas más comunes para la búsqueda de información es la búsqueda de palabras claves dentro de todos los datos que se poseen. Es por eso que es importante ir recabando estas palabras durante todo el

proceso de la investigación para que esta sirva para buscar datos correlacionados a esas palabras.

Otra técnica que puede dar mucha información es la extracción de metadatos. En donde se puede encontrar información acerca de los datos – autor, fecha de creación, fecha de modificación, última actualización…- Esta técnica puede proporcionar mucha información sin embargo existirán ocasiones en las que no es recomendable aplicarla como primera técnica para el análisis debido a la gran cantidad de datos que se requiere analizar.

En algunos casos esto es imposible, pues no se contaría con el tiempo suficiente para poder analizar cada uno de ellos. Este es uno de los retos a los que se enfrenta el cómputo forense.

Es por esta razón que se han tenido que desarrollar nuevas técnicas para la búsqueda de datos dentro de almacenamientos masivos.

Algunos ejemplos de estas técnicas son:

- El análisis estadístico en donde se propone tomar una muestra de los datos obtenidos y analizar sólo esa muestra.

- La minería de datos que consiste en la correlación de datos que genere una hipótesis. Esta técnica permite explorar grandes bases de datos con el objetivo de encontrar patrones repetitivos, tendencias o reglas que expliquen algún comportamiento.

Una vez que se cuenta con información derivada de la aplicación de métodos y técnicas de análisis es necesario ubicar esta información como hechos dentro de una línea del tiempo.

La línea de tiempo ayudará no sólo a la organización de la información sino que será un material visual que ayude al analista forense a encontrar rangos de tiempo donde hay que indagar más.

Al tener un rango de tiempo definido, el campo de estudio se reduce y esto ayuda a descartar lugares de búsqueda, centrándonos sólo en aquellos lugares clave.

Además de ubicar los datos dentro de una línea de tiempo, se deben de correlacionar los datos encontrados para que estos vayan teniendo sentido y ayuden a la reconstrucción de los hechos.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo del análisis son:

- Lista de palabras clave.
- Técnicas y herramientas para la extracción de metadatos.
- Métodos de análisis estadístico.
- Análisis por medio de minería de datos.
- Línea de tiempo.

3. *Recuperación.* Dentro de la recuperación de información se encontrarán todas las técnicas y métodos que tengan que ser aplicados cuando se posean datos ocultos o eliminados.

   Se hace necesario la aplicación de este tipo de técnicas cuando se identifica que algunos archivos han usado técnicas de cifrado, esteganografía o cualquier otra técnica para ocultar información, y la información que contengan sea relevante al caso.

También se puede encontrar que la información se encuentra protegida por algún mecanismo de seguridad, el cual no permite su acceso. En este caso antes de emplear cualquier técnica para poder acceder a la información, es necesario contar con el permiso para hacerlo, de otro modo se estaría incurriendo en un delito.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de la recuperación son:

- Técnicas de estegoanálisis.
- Editores hexadecimales.

Dentro de la fase de análisis es indispensable contar con protocolos que garanticen la integridad y confidencialidad de la evidencia. Estos protocolos deberán de ser seguidos por toda aquella persona que tenga contacto con la evidencia. Hacer uso de reglas también beneficiará a la conservación de la cadena de custodia.

La conservación de la integridad es un requisito fundamental para que la investigación tenga validez. Conservar la confidencialidad es muy importante ya que se estará en contacto con información sensible como pueden ser las vulnerabilidades del sistema, sistemas y aplicaciones que utiliza, información de los usuarios etc.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de prevención y como fue cubierta cada etapa *(Véase tabla 4.9)*.

Tabla 4.9 Preguntas clave, etapas y herramientas de la fase de análisis.

Fase de Análisis

	Preparación	Análisis	Recuperación
Preguntas claves		¿Es un dato clave?	
Etapas	• Equipo de hardware y software • Información previa	• Búsqueda de datos	• Extracción de datos
Herramientas	• Equipo de hardware y software para realizar el análisis. • Equipo para preservar la evidencia integra. • Laboratorio forense. • Lista de palabras claves.	• Lista de palabras claves. • Técnicas y herramientas para la extracción de metadatos. • Métodos de análisis estadístico. • Análisis por medio de minería de datos. • Línea de tiempo.	• Técnicas de estegoanálisis. • Editores hexadecimales

4.7 Fase Creación del Reporte.

Esta fase tiene como objetivo la creación del reporte en el que se describirá cada una de las acciones llevadas a cabo durante la identificación, preservación y análisis de la evidencia, responderá a las interrogantes de las partes así como de la autoridad y sus conclusiones de los hechos.

Para lograr este objetivo se realizan las actividades que se muestran a continuación *(Véase fig. 4.13)*.

Figura 4.13 Fase de Creación del reporte.

La fase de creación del reporte es una fase que debe de irse desarrollando conforme va avanzando la investigación. Realizar el reporte mientras se hace la investigación garantiza que no se olviden detalles y que la creación del reporte no se vuelva una tarea pesada.

El reporte se conforma con información de las fases de identificación, adquisición de evidencia y análisis.

1. *Reporte de la fase de identificación.* El reporte deberá de contener una breve reseña de cómo fue enterado el analista forense del caso, la descripción de cómo se encontró el dispositivo contenedor de la evidencia y la evidencia, y datos adicionales que haya obtenido antes de hacer la adquisición de la evidencia.

   Para documentar lo encontrado en la escena del crimen es posible anexar fotografías, planos, esquemas, dibujos y videos.

2. *Reporte de la fase de Adquisición de evidencia.* Se debe describir dentro del reporte el procedimiento que se siguió para realizar la adquisición de evidencia, en que equipos se almacenó la evidencia y que mecanismos se implementaron para garantizar su integridad.

   Es importante que se mencione el momento en el que se estableció la cadena de custodia mencionando todos sus detalles – persona responsable, la fecha y hora en la que tuvo contacto con la evidencia, acciones que realizó con la evidencia, la fecha y hora en la que dejó la evidencia a cargo de alguien más. -

3. *Reporte de la fase de análisis.* Todo el proceso de análisis – las pruebas hechas a la evidencia, métodos y herramientas utilizadas y los resultados - tendrán que ser documentado dentro del reporte.

   Al tener documentado todo el proceso de análisis seguido por el/los analistas forenses se garantiza que cualquier persona que desee comprobar los resultados pueda hacerlo siguiendo el procedimiento descrito en el reporte e invariablemente llegará a los mismos resultados.

   Es importante que se describa como fue protegida la evidencia durante el proceso de análisis y comprobar que ésta no se vio alterada por ninguna prueba a la que haya sido sometida.

Al documentar esta fase es admisible la presentación de capturas de pantalla que sirvan como apoyo de la documentación.

4. *Dar respuesta a las interrogantes de las partes y de la autoridad.* Hay veces en las que las partes o la misma autoridad elaboran cuestionarios con los puntos que les interesa aclarar para poder dar un veredicto del caso. En este caso, el analista se ve obligado a dar respuesta a estos cuestionamientos y respaldar cada una de las preguntas, con fundamento en los hallazgos que haya obtenido del análisis.

5. *Elaboración de conclusiones.* Al final del reporte, el analista da sus conclusiones respecto del caso, las cuales estarán realizadas con base en la investigación realizada del caso y en su experiencia.

6. *Validación con un abogado.* Es importante que el reporte final siempre sea validado por un abogado antes de entregarlo ante la autoridad, esto es con la intención de validar que no están incluyendo respuestas de carácter interpretativo, presuncial y/o legal

Los elementos de forma que debe de poseer el reporte son:

- Dirigido a la autoridad a cargo del asunto.
- Incluir la fecha de entrega.
- Descripción de la metodología aplicada.
- Descripción detallada de los bienes informáticos analizados.
- Descripción de visitas realizadas.
- Respuesta a los cuestionarios de ambas partes.
- Conclusiones.
- Manifestación bajo juramento de decir la verdad.
- Glosario técnico.
- Anexos físicos y lógicos.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de esta fase son:

- Editores de texto.
- Capturas de pantalla.
- Fotografías.
- Videos.
- Planos.
- Contratos, protocolos (dados por la entidad).
- Documentación que certifique el establecimiento y seguimiento de la cadena de custodia.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de creación del reporte y como fue cubierta cada etapa *(Véase tabla 4.10)*.

Tabla 4.10 Preguntas clave, etapas y herramientas de la fase de creación del reporte.

Fase de Creación del reporte	
Preguntas claves	• ¿La información sirve para comprobar los resultados? • ¿La información sirve para comprobar la integridad de los datos?
Etapas	• Reporte de la fase de identificación • Reporte de la fase de adquisición de evidencia • Reporte de la fase de análisis • Dar respuesta a las interrogantes de las partes y de la autoridad. • Elaboración de conclusiones. • Validación con un abogado.
Herramientas	• Editores de texto • Capturas de pantalla • Fotografías • Videos • Planos • Contratos proporcionados por la entidad • Protocolos de la entidad • Documentación que certifique el establecimiento y seguimiento de la cadena de custodia

4.8 Fase de Retroalimentación y Devolución de Evidencia.

Esta fase tiene como objetivo aportar recomendaciones para la mejora del sistema y hacer la devolución de datos garantizando que el analista no se quedará con ningún tipo de información.

Para lograr este objetivo se realizan actividades que ayudan a este propósito *(Véase fig. 4.14)*.

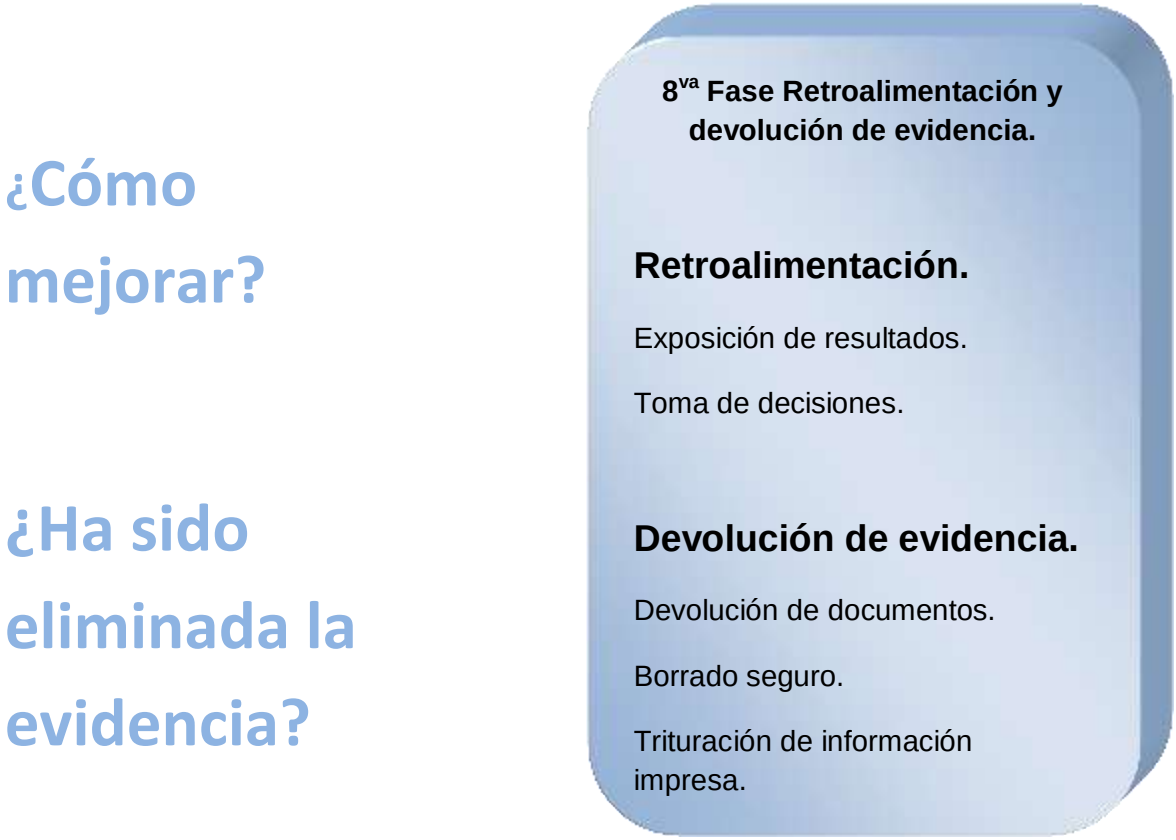


Figura 4.14 Fase de Retroalimentación y devolución de evidencia.

1.10.1 Retroalimentación.

Las actividades que se proponen para realizar una retroalimentación de los resultados, se proponen sólo si el equipo de cómputo forense es parte de la entidad afectada, es decir, trabaja como un departamento más que cuida de los activos de la entidad.

Al hacer una retroalimentación de los resultados con los demás departamentos se podrían lograr mejoras en el sistema afectado y evitar posteriores incidentes del mismo tipo.

1. *Exposición de resultados.* Se recomienda la realización de reuniones con el personal que se involucró para darle solución al incidente, por ejemplo: podría ser el equipo de respuesta a incidentes y el equipo de cómputo forense.

   En estas reuniones se deberá hacer la exposición de los resultados obtenidos, para mostrar al personal cuáles fueron las técnicas utilizadas para vulnerar el sistema y quiénes fueron los responsables.

   Al hacer el análisis de este tipo de información se podrán encontrar soluciones para mejorar el sistema ya sea desde la reestructuración del sistema o la implementación de nuevas reglas para el uso del mismo.

   Una vez acordados los cambios necesarios que deberían de hacerse para lograr una mejora y evitar posibles incidentes del mismo tipo se llevarán ante la alta gerencia.

2. *Toma de decisiones.* Sera responsabilidad de la alta gerencia analizar y evaluar las propuestas hechas para la mejora del sistema.

   Una vez realizada la evaluación de las propuestas será posible la toma de decisiones y la puesta en acción de las mismas.

1.10.2 Devolución de Evidencia.

En cuanto se abre una investigación de cómputo forense se adquiere evidencia. Evidencia que debe ser eliminada o regresada, una vez que termine el proceso legal. Garantizando a la entidad que el analista forense, no se quedará con ningún dato que le haya sido proporcionado.

1. *Devolución de documentos.* Todos aquellos documento – planos, protocolos, contratos, esquemas…- que hayan sido entregados por la entidad deberán de ser regresados.

2. *Borrado seguro.* Se deberán aplicar técnicas, ya sean físicas o lógicas, para conseguir la eliminación de los datos.

   El borrado físico de los datos se puede realizar por medio de la destrucción física de los dispositivos, éste usualmente se realiza a través de trituradoras que reducen a pequeñas piezas los medios. También se puede conseguir el mismo resultado, mediante la utilización de agentes químicos o bien la cremación. Esta técnica suele ser usada, sobretodo en medios no re-escribibles, puede ser rápida y efectiva, la gran desventaja es que el medio queda inutilizable.

   El borrado lógico se hace mediante la sobre-escritura del medio, la forma de realizarlo puede variar. Existen varios métodos para sobre-escribir el medio, algunos son más seguros que otros. Las ventajas de utilizar esta técnica es que se puede realizar de manera remota y de manera simultánea sobre varías medios y que el medio no queda inutilizable.

3. *Trituración de información impresa.* En caso de que el analista contara con información impresa del caso que no debiera ser devuelta a la entidad, deberá deshacerse de esa información.

La forma más común de eliminar esta información es triturándola en máquinas trituradoras de papel. Existen varios tipos de estas máquinas, se recomienda el uso de aquellas que hacen más de un tipo de corte a la hoja, porque la recuperación del documento se hace más complicada.

Herramientas:

Las herramientas que se pueden utilizar para cumplir el objetivo de esta fase son:

- Técnicas para hacer el borrado seguro de datos.
- Equipo de software que garanticen el borrado seguro de datos.
- Equipo de hardware que garantice el borrado seguro de datos.
- Trituradora de papel.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de retroalimentación y devolución de evidencia y como fue cubierta cada etapa *(Véase tabla 4.11)*.

Tabla 4.11 Preguntas clave, etapas y herramientas de la fase de retroalimentación y devolución de evidencia.

Fase de Retroalimentación y devolución de evidencia		
	Retroalimentación	**Devolución de la evidencia**
Preguntas claves	• ¿Cómo mejorar? • ¿Ha sido eliminada la evidencia?	
Etapas	• Exposición de resultados • Toma de decisiones	• Devolución de documentos • Borrado seguro • Trituración de información empresa
Herramientas	• Técnicas para realizar borrado seguro de datos • Equipos de software que garanticen el borrado seguro de datos • Equipo de hardware que garantice el borrado seguro de datos • Trituradora de papel	

5. Análisis de la Metodología Propuesta.

La aplicación de esta metodología, trae como ventaja sobre las otras metodologías, que es aplicable para cualquier tipo de tecnología y en cualquier tipo de dispositivo que almacene evidencia de forma digital.

Esta metodología toma en cuenta los retos a los que se enfrenta el cómputo forense, por lo cual propone diferentes técnicas y mecanismos para el tratamiento

de grandes volúmenes de información y para el tratamiento de archivos que contengan información oculta.

Además de proponer una fase de prevención en la que se podrá hacer un análisis previo de los sistemas que se atenderán, en el caso de que el analista forense se encuentre encargado de dar respuesta ante algún sistema en específico.

En el caso de que el analista tenga que responder ante cualquier tipo de sistema en esta fase será donde se actualice a cerca de las nuevas tecnologías, técnicas y métodos usados para el almacenamiento de información, ocultamiento de datos y tratamiento de información, además de aprender de los sistemas que haya analizado con anterioridad.

También hace la propuesta de una fase completamente dedicada a regresar la evidencia a la entidad que la proporcionó. Este es un punto importante sobre todo para la entidad que proporciona información. Realizar el borrado seguro de la información, le asegura a la entidad que el analista forense no se quedará, ni distribuirá la información que se le haya facilitado.

Esta metodología cuenta con ocho fases para su desarrollo, en las cuales se incluyen todos los pasos generales que debe de contener una metodología de cómputo forense para dar respuesta ante un incidente de seguridad.

A continuación se muestra una tabla que contiene las fases que componen la metodología forense y las etapas que debe de contener una metodología forense *(Véase fig. 4.12).*

Tabla 4.12 Análisis de la metodología propuesta.

Etapas generales de una investigación forense	**Metodología propuestas**							
	Prevención	Identificación	Preparación	Adquisición de evidencia	Preservación	Análisis	Creación del reporte	Plan de retroalimentación
Identificación		✓						
Preservación			✓	✓	✓			
Análisis						✓		
Presentación							✓	

En esta tabla se puede ver que la metodología de cómputo forense propuesta cumple con todas las fases que debe de contener una metodología forense

En el siguiente capítulo se desarrollará un caso práctico de una investigación forense real que se realizó en el Laboratorio de Seguridad Informática de la FES Aragón en la que se implementó la metodología forense propuesta en este trabajo.

Capítulo Quinto
Metodología propuesta aplicada a un caso práctico.

En este capítulo se presentará un caso real de una investigación de cómputo forense desarrollada en el Laboratorio de Seguridad Informática que se encuentra a cargo del M.C Leobardo Hernández Audelo.

El caso se desarrollará bajo la metodología propuesta en este trabajo de tesis *(Véase Capítulo cuarto)* dividiendo el trabajo realizado en las ocho fases que propone la metodología –prevención, Identificación, preparación, adquisición de la evidencia, preservación, análisis, retroalimentación y devolución de la evidencia-.

Al presentar el desarrollo de la investigación se omitirán los nombres de la entidad afectada y se mantendrá en anonimato a las personas involucradas.

1. Introducción al caso práctico.

El día miércoles 2 de abril de 2008 se reporta en una sucursal bancaria 45 depósitos para abono en diversas cuentas de las cuales no se recibió el dinero en efectivo. Estos movimientos se registraron bajo la cuenta 1101 cuenta que pertenece a una cajera a la cual llamaremos cajera1, la cual trabajaba en la ventanilla 1 de la sucursal identificada en el sistema como la terminal MR07.

Se encontró que de los 45 depósitos realizados 40 requirieron de la autorización del subgerente a cargo, al cual nombraremos como subgerente. Dichos movimientos bancarios se registraron a partir de las 9:39:41am y hasta las 10:48:37am.

El día martes 6 de Mayo de 2008 la institución bancaria informa a su representante que el sugerente y la cajera1, desde el día 5 de Mayo de 2008 faltaron de manera injustificada, a laborar, por lo cual la institución bancaria se dio a la tarea de localizarlos mediante la consulta de los movimientos que estas personas pudieran haber realizado con sus tarjetas de débito proporcionadas por el mismo banco, cuentas en donde les era depositado su salario.

Al realizar estas consultas detectaron que el día 5 de Mayo el subgerente y la cajera1 realizaron retiros de sus cuentas desde otro estado, se hace la consulta de la secuencia de vigilancia de la cámara instalada al interior del cajero automático, donde se puede apreciar al subgerente y a la cajera1, haciendo en el mismo momento operaciones de retiro de dinero en el cajero. Hecho por el cual se formula la denuncia y/o querella en caso de que se considere necesaria, en contra del subgerente y la cajera1, haciendo énfasis en que estos han abandonado su lugar de trabajo, teniendo conocimiento de las investigaciones practicadas por el Grupo Financiero, el cual los hace responsables de las operaciones ilícitas.

Los servicios del Laboratorio de Seguridad fueron requeridos por parte de la cajera1, quien fue acusada de cometer las operaciones ilícitas junto con el subgerente.

La investigación inicia una vez que la cajera1 solicita, la ayuda del Laboratorio de Seguridad Informática de la FES Aragón y la intervención del M.C Leobardo Hernández Audelo, como perito en informática.

La investigación inicia desde la fase de Identificación, ya que la fase anterior –fase de prevención- dado que se trata de una investigación a una entidad completamente ajena, no se tenían previos conocimientos de su funcionamiento, sistemas, protocolos, etc. Que se puedan documentar. Sin embargo la continua actualización es algo que se practica en el Laboratorio de Seguridad Informática día con día.

2. Fase de Identificación.

Cuando la cajera1 solicita la ayuda del Laboratorio de Seguridad Informática, por ser ella el primer acercamiento con el caso, se le pide que relate cómo sucedieron los hechos el día 2 de Abril de 2008.

La versión de la acusada es la siguiente. El día 2 de Abril de 2008 ella se presentó a trabajar como solía hacerlo, entrando ese día a las 8:07:44 am y se autenticó en el sistema para que este registrara que la caja estaría siendo atendida por la cajera1, que dentro del sistema se registra con el numero 1101. Comenta que mientras hacia su trabajo la máquina que saca los comprobantes de depósito empezó a arrojar varios comprobantes sin que ella los hubiera marcado en la máquina como movimientos. Dio aviso a su supervisor y explicó lo que había

sucedido, a lo cual él le comentó que lo revisarían después, que por lo mientras continuara desarrollando sus actividades y al final del día verían como resolver ese problema.

Al finalizar el día el supervisor le dijo que iban a levantar un reporte y que habría una investigación para saber qué fue lo que pasó. Después de dos días el supervisor le dijo a la cajera1 y al subgerente que fueran a otra sucursal porque ahí resolverían lo del problema de los comprobantes. Así también comenta que el supervisor les informó que se les abonaría dinero en sus cuentas para que pudieran realizar el viaje y solventar los gastos.

Ellos cumplieron y se trasladaron a la sucursal indicada, cuando llegaron les dijeron que tendrían que esperar y que posiblemente necesitarían permanecer en ese estado algunos días, para lo cual ellos decidieron retirar dinero de sus cuentas, fue entonces cuando los detuvieron diciéndoles que había una orden en su contra.

Desde este momento podemos ir recabando palabras claves que nos ayudarán durante todo el proceso de la investigación forense *(Véase fig. 5.1)*.

Lista de palabras clave

El nombre de los acusados: cajera1 y subgerente

El numero de usuario del cajero: 1011

El número de usuario del subgerente: 3003

Número de cuentas afectadas: 45

Número de cuentas que requirieron autorización del subgerente: 40

Hora de registro del primer movimiento irregular: 9:39:41 am

Hora de registro del último movimiento irregular: 10:48:37 am

Caja desde la cual se realizaron los movimientos: Caja1

Fecha de registro de los movimientos: 2 de abril de 2008

Terminal: MP07

Figura 5.1 Lista de palabras clave.

Se realizaron preguntas a los acusados para conocer cómo era la operación del sistema que utilizaban diariamente. Así fue como supimos que para poder operar el sistema AS –sistema que operaba como cliente- cada usuario tenía que introducir un usuario y contraseña valida, con lo cual el sistema registraba que las operaciones siguientes estaban bajo el cargo del usuario que había establecido conexión.

Una vez que accedían al sistema podían realizar diversos movimientos bancarios. En el caso de los depósitos, estos podían ser realizados por el cajero en turno, pero si el depósito era de más de $100 000 pesos éstos tenían que ser autorizados por el subgerente de la sucursal.

Todos los registros de los movimientos bancarios eran almacenados, tanto en el equipo desde el cual se habían ejecutado –el equipo ubicado en cada

ventanilla-, como en un servidor que almacenaba el registro de los movimientos bancarios realizados en las diversas sucursales.

También se pudo conocer que el día en que sucedieron los hechos -2 de Abril de 2008- se encontraba el sistema de video encendido, el cual debería mostrar lo que ellos aseguran que pasó.

Con base en la información proporcionada se formulan hipótesis de lo que pudo haber sucedido en el sistema.

La primera hipótesis que se puede vislumbrar es que la máquina que operaba la cajera1, haya podido ser accedida de forma remota. Esto se intuye porque la cajera1 dice que repentinamente sin haber ejecutado una instrucción previa la máquina que entrega los comprobantes de operaciones empezó a arrogar bauchers.

Si es que la ejecución de los movimientos bancarios vino por parte de un tercero, entonces se tendrían que haber visto comprometidas las contraseñas de la cajera1 y del subgerente, ya que estas eran necesarias para poder realizar alguna operación bajo su nombre y número de usuario.

Siguiendo esta hipótesis se solicita a la institución, a través de un cuestionario de tres puntos, información acerca de la institución, del sistema y su administración, de la construcción de contraseñas y de los videos tomados por el sistema de circuito cerrado con el que cuenta la sucursal en donde se registraron los movimientos irregulares[22], así como el permiso para entrar a las instalaciones, acceder al equipo involucrado, y ver una demostración de cómo funciona el sistema tanto de la parte del cliente como del servidor.

[22] Se les llama irregulares ya que los depósitos se registran en el sistema como depósitos en efectivo sin que exista la entrada de dinero a la caja.

A continuación se presentan las trece peticiones que se le hacen a la institución bancaria.

1. Todas las bitácoras del sistema AS correspondientes al día 2 de Abril de 2008, tanto de la parte del aplicativo cliente como del servidor (core), en formato digital.

2. Documentación de operación y administración del sistema AS tanto de la aplicación cliente como de la aplicación servidor (core), del tipo de red que se utiliza en el caso y del lenguaje de programación en que se encuentra desarrollada la aplicación AS.

3. Información sobre la versión del sistema AS, del sistema operativo sobre el cual se ejecutan tanto el cliente como el servidor (core).

4. Documentación correspondiente del diseño y arquitectura de seguridad del sistema AS en su esquema integral cliente-servidor.

5. Documentación sobre los controles y mecanismos de seguridad implementados tanto en el sistema AS como en el sistema operativo y de la red sobre la cual se ejecutan tanto el cliente como el servidor (core).

6. Documentación sobre el tipo de contraseñas (construcción) permitidas por el sistema, la forma en que se almacenan, forma en que se trasmiten por la red y forma en que se validan dichas contraseñas para realizar el proceso de autenticación del usuario y la autorización de las transacciones.

7. Copias certificadas de los resultados de las Autoridades de la Comisión Nacional Bancaria y de Valores realizadas a la institución bancaria sobre el sistema AS y sistemas relacionados durante el año 2008 y en su caso 2007.

8. Información explicita sobre los estándares de seguridad, nacionales e internacionales con los que cumple el sistema bancario AS para evitar el robo de entidad.

9. Documentación sobre la administración del sistema y nombres de los responsables de la administración del mismo sistema. Facilidad para entrevista del perito con el administrador o administradores del sistema.

10. Código fuente y ejecutables de la aplicación, tanto del servidor (core) como del cliente y de todo código necesario para realizar el análisis de la funcionalidad y seguridad del sistema.

11. Recreación presenciada por el perito, del sistema AS en su operación normal desde su inicialización, operación y baja o bloqueo del mismo, tanto del cliente como del servidor (core).

12. Acceso a las instalaciones de la institución bancaria donde se localiza la aplicación cliente, la aplicación servidor y acceso al equipo de cómputo involucrado en el caso. Igualmente en las misma instalaciones, acceso a verificar la posición de las cámaras del circuito cerrado (CCTV) y la operación de las mismas.

13. Los videos correspondientes a las grabaciones de la cámara (CCTV) del día 2 de Abril de 2008 e información sobre los mecanismos de verificación de integridad usados para no permitir la edición y alteración de los mencionados videos.

La institución bancaria en respuesta al punto uno dio las bitácoras de acceso al sistema AS, la cual fue extraída del espacio no asignado del servidor de la sucursal.

A la petición hecha en el punto dos la institución bancaria respondió de la siguiente manera “la documentación entregada corresponde a los depósitos de sistema AS, ya que es la que será relevante para el caso que nos ocupa. Lo anterior debido a que por razones de seguridad, ya que de ello depende la información de una gran cantidad de clientes, y hacer uso de la misma revelaría información protegida por la Ley de Instituciones de crédito”

Proporciona el proceso para el depósito de cuentas, el cual se encuentra descrito en las tablas, donde se muestran las diferentes actividades consecutivas que tienen que realizar los cajeros para poder hacer un depósito.

Con respecto al tipo de red, informan que el tipo de red utilizado corresponde a SNA (Systems Network Architecture) arquitectura de red diseñada y utilizada por IBM para la conectividad con sus hots o mainframe grandes ordenadores y servidores muy robustos, servidores meddlerange. El servidor Host Integration Server que corriendo en Microsoft Windows Server, funciona como Gateway entre la red de mainframes en SNA y una red TCP/IP con Windows.

Esta arquitectura de red, es comúnmente utilizada por bancos por considerarse más seguro que TCP/IP.

También se les solicitó en ese mismo punto información acerca del lenguaje de programación a lo que contestaron que “La aplicación As utilizada, está desarrollada en un lenguaje de programación “CT (Consumer Transaction)”

En el punto tres se les solicitó que proporcionaran información sobre la versión del sistema AS del sistema operativo sobre el cual se ejecutaba tanto la aplicación cliente como el servidor (core)

A lo que contestaron que la versión AS vigente al momento del incidente corresponde a la versión 38.5 y la versión del sistema Operativo Core OS/390.

En el punto cuatro se solicitó información acerca de diseño y arquitectura de seguridad del sistema AS en esquema integral cliente-servidor. Para responder a esta petición entregaron un esquema del funcionamiento cliente – servidor.

En el punto cinco se solicitó documentación sobre los controles y mecanismos de seguridad implementados tanto en el sistema _AS como del sistema operativo y de la red sobre la cual se ejecutan tanto el cliente como el servidor (core).

Esto fue lo que se obtuvo de respuesta “Los siguientes controles están implementados en el servidor core y cuentan en algunos casos con su contraparte implementada en el sistema AS”

Controles de inicio y cierre de operaciones en sucursales.

Validación y registro de eventos en apertura y cierre de cada sucursal.

Registro central de operaciones (usuario y operación).

Control de operación en días festivos y fines de semana.

Validaciones de sucursal al inicio de operación de cada cajero.

Control de cierre de sucursal en forma local hasta el cierre de cajeros y usuarios.

Bloqueo de operaciones al cierre de la sucursal.

Registro central de reportes de cierre.

Registro en Logs:

- Eventos.
- Operaciones.
- Catálogos de sucursales.
- Días festivos por plaza.
- Terminales por plaza y sucursales.
- Explotación de Logs (Reportes de control).

Controles de usurario.

Registro en logs de altas y bajas y cambios de usuario

Operaciones en Core para inicio, salida provisional y Cierre de caja.

Relación entre usuarios y número de empleado (validación de empleados y estado del mismo).

Funciones:

- Alta de usuarios.
- Baja de usuarios.
- Baja temporal de usuarios (por vacaciones o incapacidad).
- Cambio de perfil.
- Inicio de cajeros en sucursales.
- Salida provisional del cajero.

- Uso de contraseñas.
- Restricción de acceso múltiple.
- Manejo de diferentes estados en usuarios.
- Validaciones de cajeros al cierre de la Sucursal.
- Perfiles de usuario por puesto.
- Registro de Logs.
- Registro central de eventos (exitosos o rechazados).
- Uso de Logs de eventos y Seguridad.
- Inicio de operaciones (usuario por sucursal).
- Explotación de Logs (Reportes de Control)

Controles de Operación:

- Diario de transacciones.
- Formatos estándares de diario de transacciones.
- Registro central de todas las operaciones de cada sucursal.
- Control de operaciones con doble firma cuando se exceden facultades.
- Identificación central de operaciones por número de registro de empleado y autorizador.
- Registro de Logs.
    - Registro central de eventos.
    - Uso de Log Operaciones Bancarias.
    - Explotación de logs (Reportes de Control).

Los controles y mecanismos de red son los provistos por el protocolo SNA.

En el punto 6 se solicitó información acerca del tipo de contraseñas (construcción) permitidas por el sistema, la forma en que se almacenan, la forma en que se trasmiten por la red y la forma en que se validan dichas contraseñas para realizar el proceso de autenticación del usuario y la autorización de transacciones.

A lo que la institución bancaria respondió: “Las contraseñas son de carácter alfanumérico. Asimismo, requieren al usuario el cambio periódico obligatorio, cuentan con longitudes mínimas máximas y se validan los caracteres repetidos. Por otro lado, las contraseñas tienen un periodo de caducidad y se obliga al usuario su cambio cuando se utiliza por primera vez.

Las contraseñas se almacenan encriptadas en base de datos y para la validación se transportan en red encriptado.

La Bitácora de contraseñas permite mantener un histórico de contraseñas, validándose que no se use la misma contraseña al caducar su vigencia.

En el punto siete se solicitaron las copias certificadas de los resultados de las auditorias de la Comisión Nacional Bancaria y de Valores realizadas a la institución bancaria sobre el sistema AS y sistemas relacionados durante el año 2008 y 2007.

La institución respondió que: “En las visitas realizadas por la Comisión Nacional Bancaria y de Valores durante los años 2007 y 2008, dicha autoridad no realizó auditorías al sistema AS ni a sistemas relacionados”

En el punto ocho se solicitó información explicita de los estándares de seguridad, nacionales e internacionales, con los que cumple el sistema bancario AS para evitar el robo de identidad.

Como respuesta se informa que: “El sistema se Seguridad AS está basado en los siguientes estándares nacionales e internacionales.

COIT (Control Objectives for Information and related Technology) conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en ingles: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (en inglés IT Governance Institute) en 1992.

En apego al COBIT, la institución considera las siguientes áreas en lo concerniente a los mecanismos y controles de seguridad.”

Planeación y organización.

- Estable las prácticas para considerar los beneficios, políticas y niveles de servicio entre otros, en cumplimiento de los objetivos del negocio.
- Permite definir una arquitectura de información para entender requerimientos de información en forma consistente y confiable.
- Apoya en la determinación de una orientación tecnológica que permita contar con una infraestructura y estándares para entender las necesidades del negocio.
- Permite obtener respuestas ágiles mediante estructuras adecuadas y con roles y responsabilidades.
- Establecimiento de canales de comunicación oportunos sobre los servicios y riesgos en TI.
- Permite contar con un marco de referencia para la evaluación y administración de riesgos.

Adquisición e implementación.

- Permita contar con soluciones automatizadas con diseño efectivo y eficiente que consideren un costo razonable y una implementación oportuna.
- Contar con una infraestructura de acuerdo con la arquitectura y estándares.
- Operar los recursos de cómputo de acuerdo con niveles de servicio con terceras partes.
- Contar con recursos apegándose a los procesos legales, arquitectura y estándares.
- Realizar los cambios a los sistemas e implementar los recursos en un marco de trabajo controlado.

Entrega y Soporte.

- Permite definir los niveles de servicio para atender los requerimientos del usuario.
- Administrar los niveles de servicio con tercera parte.
- Contar con mecanismos que permitan la continuidad del servicio y que aseguren el nivel de seguridad en las aplicaciones.
- Definir controles para la administración de la configuración, manejo de fallas, manejo de datos, seguridad física y ambiental, así como la administración de operadores.

Monitoreo y evaluación.

- Estos procesos permiten contar con indicadores de desempeño para reportar sistemática y oportunamente las desviaciones para tomar acciones oportunas
- Permite monitorear el alineamiento de las actividades con las directrices y políticas

NIST (National Institute of Standard and Technology), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este Instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y calidad de vida. En relación con prácticas de seguridad se consideran los siguientes estándares

- **800-13** Telecomunication Security Guidelines for Telecommunications Management Network
- **800-14** Generally Accepted Principles and Practices for Securing Information Technology Systems.
- **800-53** Recommended Security Controls for Federal Information Systems.
- **800-100** Information Security Handbook: A Guide for Managers.

Autoridades Mexicanas, múltiples leyes para la correcta y segura administración de los fondos de la clientela como:

- Ley de Instituciones de Crédito (LIC)- Protección des secreto bancario y fiduciario.
- Seguridad en el uso de medios electrónicos (Disposiciones de la LIC).

- Disposiciones de Control Interno (Disposiciones de la LIC).
- Lineamientos mínimos de operación y seguridad para la contratación de servicios de apoyo tecnológico.
- Circular única de bancos- Administración de Riesgos Tecnológico.
- Circular única de sociedades de inversión- Administración de Riesgo Tecnológico.

DES (Data Encryption Standard) algoritmo criptográfico utilizado para la protección de las contraseñas en el Sistema AS. DES evita su divulgación no autorizada.

DES es un sistema de criptografía de llave simétrica que fue concebido en 1972 como una derivación del algoritmo Lucifer desarrollado en IBM por Horst Feistel. DES describe el algoritmo de encriptación de datos DEA (Data Encryption Algorithm) y es el nombre que adoptó en 1977 de FIPS (Federal Information Processing Standard) 46-1 [Data Encryption Standard, FIPS PUB 46-1, Washington, D.C,. National Bureau of Standards, 15 de Enero de 1977]. DEA es también definido como el Standard ANSI X3.92 American Nacional Standard for Data Encryption Algorithm, [American Nacional Standards Institude, 1981]. DES recibió su certificación en 1933 de NIST (Nacional Institute of Standards and Technology).

DEA utiliza bloques de datos de 64 bits y una llave de 56 bits, con esta longitud de llave se tendría que probar 2 elevado a las 56 posibles llaves (72,057’594,037’927,936) en un ataque de fuerza bruta.

DES opera en 4 diferentes modos:

- Cipher Block Chaining (CBC).
- Electronic Code Book (ECB).

- Cipher Feedback (CFB).
- Output Feedback (OFB).

ISF (Information Security Forum), organización internacional independiente dedicada al benchmarking y las mejores prácticas en materia de Seguridad de la Información. Establecida en 1989, cuenta con cientos de miembros a nivel mundial.

En apego **"The Standard of good practice for Information Security"** de la ISF Scotiabank Inverlat tienen implementados los siguientes controles y mecanismos de seguridad:

- Las pautas de conducta para tecnologías de TI prohíben que se comprometan las contraseñas (por ejemplo se prohíbe a los empleados bancarios escribirlas o revelarlas a otros).
- La gestión de acceso e identidad provee un conjunto consistente de métodos para: a) identificar a los usuarios a través de identificadores de usuario únicos; b) autenticar usuarios a través de la contraseña; c) uso de un proceso de firma (sign-on); autorización de privilegio de acceso a los usuarios; d) administración de los privilegios de acceso a usuarios.
- El core está configurado para el cambio de parámetros relacionados con la seguridad para que sean diferentes a los valores por omisión del proveedor.
- Apego al principio "El acceso a la aplicación e información asociada debe restringirse a individuos autorizados".
- Los usuarios de la aplicación se: a) identifican a través de un identificador de usuario único; b) autentican través de una contraseña y c) se proveen con la funcionalidad mínima requerida para llevar a cabo su función.
- Existe un proceso para emitir nuevas contraseñas que aseguran que la revelación de contraseñas se minimiza cuando se comunican al usuario, forzando al usuario al cambio de contraseña cuando se usan por primera

vez. Adicionalmente asegura que las contraseñas se cambian regularmente.

- El acceso a la aplicación se graba en bitácoras.
- Programa de consciencia de seguridad en las Pautas de Conducta dirigida a los usuarios.
- Todos los usuarios deben obtener previamente una autorización antes de que obtengan acceso a los recursos.
- Los privilegios de acceso no se asignan de manera colectiva (por ejemplo, identificadores de usuario son únicos); a) aseguran que las contraseñas no se despliegan en la pantalla ni se imprimen; b) emisión de contraseñas temporales a los usuarios que deben cambiarse al primer uso; c)forzar que las nuevas contraseñas tienen un número mínimo de caracteres de longitud, difieren de su identificador de usuario asociado; d) asegurar que los usuarios eligen su propia contraseña; e) asegurar que las contraseñas se cambian regularmente; f)restringir el reusó de contraseñas.

En el punto nueve se solicitó la documentación sobre la administración del sistema y nombre de los responsables de la administración del mismo sistema.

Como respuesta a esta petición la institución respondió que:

“La Seguridad en AS, es un conjunto de elementos de control que se implantan para proteger los programas y la información, que son procesados y almacenados por medio de los sistemas de cómputo. La institución bancaria tiene implementadas las siguientes políticas para la administración del sistema:”

Relativo al empleado del Banco.

- El acceso a los sistemas y el manejo de la información a su cargo debe ser únicamente orientado al desempeño de las funciones que correspondan al puesto que tiene asignado.
- No debe de proporcionar su contraseña ni el número de usuario, a ninguna otra persona, por seguridad y ser estrictamente de carácter personal, ni aun cuando tenga que ausentarse por cualquier motivo de su trabajo (vacaciones, incapacidad o enfermedad, etc.).
- Su uso está sujeto a lo establecido en las “Pautas de Conducta en los Negocios” del Grupo de la Institución bancaria.
- El cumplimiento a la Normatividad será motivo de amonestación de las sanciones señaladas en el Reglamento Interior de Trabajo.

Uso de las claves de acceso al Sistema.

Las claves son exclusivamente de uso individual y permiten tener acceso a las aplicaciones del Sistema de Automatización de Sucursales (AS).

El Subgerente de Servicio / Supervisor responsable verifica que:

- Todos los usuarios firman la carta responsiva / de resguardo emitida por el sistema de AS, por:
  - Alta.
  - Baja por: cambio de sucursal / puesto, renuncia.
  - Cambio de contraseña (en cambio por olvido).
  - La carta responsiva / de resguardo, se guarde.
  - En el expediente del empleado de la sucursal.

- En un expediente creado para el personal de apoyo, en su caso.
- El responsable de la clave de acceso al sistema la cambie por seguridad.
- En el caso del sistema AS (lo solicita en forma automática).
- Al salir y regresar de vacaciones o incapacidad.
- Cuando existe la sospecha de que la clave de acceso al sistema es de conocimiento de otra persona.

El personal de sucursales, debe cambiar periódicamente su clave asignada en el sistema de AS.

El gerente de Sucursal / Supervisor responsable, supervisa que:

- Las claves usuarios para la Seguridad del Sistema de AS, estén asignadas a los puestos.
- Se depuren en el Administrador del Sistema, los usuarios de la Sucursal cuando el empleado:
  - Disfrute de vacaciones.
  - Se encuentre de incapacidad.
  - Sea reasignado a otro puesto / sucursal.
  - Se separe de la Institución.

Clave de Subgerente de Servicio del Sistema AS.

Las claves de acceso confidencial de Subgerente de Servicio están homologadas con las facultades individuales de autorización otorgadas a cada puesto, es responsabilidad del funcionario que tiene asignada la clave de

Subgerente de Servicio, utilizarla de acuerdo con el límite establecido en sus facultades de autorización

Las estaciones de trabajo solicitan clave de Subgerente de Servicio, en transacciones de depósitos, por los importes definidos para la Autorización Operativa.

Confidencialidad de las claves.

Todos los empleados del Banco son responsables de:

- Mantener la confidencialidad de su clave de Seguridad que les fue asignada, tanto para accesar al Sistema de AS, como para otorgar clave de Supervisor.

Lineamientos

- Los sistemas de control de acceso deben estar configurados y protegidos para garantizar su continua Integridad y Disponibilidad.
- Las configuraciones y parámetros del software de Acceso están adecuadamente configurados para satisfacer los requerimientos que se están procesando.
- Los sistemas de control de acceso lógico se deben mantener vigentes y deben cumplir con los requerimientos del Grupo Financiero.
- Deben de existir planes para garantizar la continuidad de todos los sistemas de control de acceso.
- Por lo menos una copia de respaldo del software de seguridad, de la información de seguridad y de los registros de actividad de seguridad del sistema deben almacenarse fuera del sitio, en un lugar seguro.

- Se debe de mantener la custodia adecuada de los privilegios de acceso.

- Todos los usuarios de un sistema de cómputo del Grupo Financiero, deben de identificarse de manera única como usuarios autorizados del sistema de cómputo de Grupo Financiero.

- A todos los usuarios se les debe hacer conciencia de sus responsabilidades de seguridad.

- Los usuarios no pueden aumentar o cambiar sus privilegios de acceso.

En el punto diez se solicitaron los códigos fuentes y ejecutables de la aplicación tanto del servidor (core) como del cliente y de todo código necesario para realizar el análisis de la funcionalidad y seguridad del sistema.

A lo que se respondió lo siguiente: “No es posible proporcionar los códigos fuentes y ejecutables de la aplicación (core), así como del cliente, debido a que dichos códigos y ejecutables permanecen en uso constante y son necesarios para sustentar la operación y los procesos del banco. Suspendes la disponibilidad de los ejecutables en uso implicaría afectar no solo la operación interna sino también los servicios proporcionados al público.”

En el punto once se solicitó la recreación, presenciada por el perito, del sistema AS en su operación normal desde su inicialización, operación y baja o bloqueo del mismo, tanto del cliente como del servidor. Y en el punto doce se solicitó el acceso a las instalaciones de la institución bancaria donde se localiza la aplicación cliente, la aplicación servidor y acceso al equipo de cómputo involucrado en el caso, así como el acceso a verificar la posición de las cámaras de circuito cerrado (CCTV) y la operación de las mismas.

A lo que la institución bancaria contestó: Nos permitimos manifestar que para la realizar la visita física a las instalaciones de la Sucursal Bancaria, tomando en consideración que se trata de una oficina Bancaria que se encuentra en operación diaria al público y con manejo de efectivo, por cuestiones de seguridad y logística se requiere que la autoridad que planea realizar la visita, informe al banco con cuando menos cinco días de anticipación la fecha exacta y hora en que se planea realizar y nombre de las personar se practicarán la diligencia, con la finalidad de poder tomar las medidas de seguridad necesarias en caso de que resulte necesario para no afectar la operación misma.

No omitimos precisar, que la diligencia deberá practicarse en días y horas hábiles (lunes a viernes de 9:00 a 16:00 horas)

De igual forma, resulta importante destacar que como parte de los procesos constantes de modernización tecnológica que a nivel mundial realiza la institución bancaria, para eficientizar la operación y el servicio que se brinda a los clientes, se desarrolló un nuevo sistema denominado PLATAFORMA INTERACTIVA DE CAJERO identificada como “ITP” por sus siglas en idioma Ingles, plataforma que está substituyendo de forma paulatina al sistema con el que anteriormente trabajaban las Sucursales del Banco conocido como “AS”, por los que desde los primeros meses del año 2009, se está ejecutando un programa de implementación del sistema “ITP” en la red de sucursales a nivel nacional, por lo que la recreación solicitada por el perito de la Defensa, deberá realizarse en las oficinas centrales de la institución bancaria, el día y hora que al efecto señale la autoridad que pretende realizar la diligencia.

Al igual que en el caso anterior, por cuestiones de seguridad y logística se requiere que la autoridad que planea realizar la visita, informe al Banco con cuando menos cinco días de anticipación la fecha exacta y hora en que se planea realizar y el nombre de las personas se practicaran la diligencia, con la finalidad de poder tomar las medidas de seguridad necesarias y permitir el acceso a las

mismas ya que se tratan de oficinas en donde se resguarda información considerada confidencial.

Digital en formato propietario y firma digital de fábrica, **que no permite editar y/o** No omitimos precisar, que la diligencia deberá practicarse en días y horas hábiles (lunes a viernes de 09:00 a 18:00 horas)"

En el punto trece se solicitaron los videos correspondientes a las grabaciones de las cámaras de CCTV del día 2 de abril de 2008 e información sobre los mecanismos de verificación de integridad usados para no permitir la edición y alteración de los mencionados videos.

Como respuesta a esta petición la institución contesto que: "Las imágenes de las cámaras son almacenadas video grabadora **alterar las imágenes.**

No obstante lo anterior, como la institución bancaria lo hizo oportunamente del conocimiento del Ministerio Público del fuero común en el Distrito Federal, al momento de rendirse el informe en materia de informática, sólo se incorporaron las secuencias que lograron obtenerse del equipo que resguardaba la información relativa a las imágenes, ya que por fallas electrónicas del equipo que concentraba la información se dañaron los archivos, por lo que materialmente estamos imposibilitados para exhibir los videos requeridos.

Sin perjuicio de ello, se insiste en que el formato que se maneja para grabar no permite **editar y/o alterar las imágenes,** lo cual no implica que no pueda dañarse el equipo que almacenaba la información, como sucedió en el presente caso.

Sin otro particular, quedamos a sus órdenes para cualquier duda o comentario adicional."

Al ver la contestaciones proporcionas por el Banco Muestra se en los puntos 11, 12 y 13 se hace la formulación de una segunda petición con cinco puntos. Estos son:

14. Solicitó copia en medios electrónicos de toda la información digital contenida en el disco o discos duros del equipo o equipos de cómputo involucrados en la operación, local o remota, del sistema o sistemas de software relacionados con las operaciones supuestamente fraudulentas, así como de las bitácoras y registros relacionados con las mismas, ya sea que éstos se encuentren en los equipos directamente involucrados o en algún otro equipo.
15. También solicito la garantía formal, cualquiera que esta sea, de que tanto la información, el software de aplicación, sistemas operativos y demás software contenido en estos equipos en el momento de sucedido el caso que nos ocupa, así como también los equipos mismos o alguna de sus partes o componentes no hayan sido cambiados o alterados ni física ni lógicamente desde el momento en que sucedió el caso hasta el momento de la diligencia que nos ocupa. De no ser así, es decir, si la información, el software o el equipo han sido cambiados o alterados, se estará dando por hecho la violación a la cadena de custodia.
16. Solicito copia en medios electrónicos de toda la información, en el formato y medio en el que se mantengan y resguarden, de los videos correspondientes a las grabaciones de las cámaras de CCTV del día 2 de abril de 2008 e información sobre los mecanismos de verificación de integridad usados para no permitir la edición y alteración de los mencionados videos.

Los puntos 14 y 16 anteriores son necesarios debido a que el análisis forense de los datos requiere de herramientas, condiciones, equipo y

laboratorio especializado que no se tiene ni se puede tener durante el desahogo de la diligencia y es necesario realizar este trabajo con posterioridad al desahogo de una diligencia mencionada

17. Solicito poder hacer las preguntas que considere importantes respecto a la operación, funcionamiento y demás aspectos técnicos respecto a los equipos de cómputo, programas de software, equipos y operaciones de la red y cajeros automáticos al personal responsable del Banco Muestra y que estas preguntas serán respondidas correctamente en concepto, tiempo y forma por el personal designado por la mencionada institución bancaria ya sea en forma oral o escrita.
18. Solicito facilidades y autorización para videograbar y fotografíar las instalaciones de la sucursal, o las partes de ella que el perito considere importantes para su peritaje, así como también para videograbar y fotografíar los equipos de cómputo involucrados y que el perito considere importantes en su peritaje.
19. Solicito facilidades y autorización para auxiliarme de una persona que me apoye en mis actividades durante el desahogo de las diligencias correspondientes. Esta persona será designada por el perito.

Al conceder el permiso para acceder a las instalaciones y al equipo involucrado se puede observar la ubicación física de las cámaras de video que permanecían prendidas en todo momento almacenando las grabaciones tomadas, la ubicación de las ventanillas y la disposición del inmueble. Para poder registrar esto se hizo la toma de un video en el cual se puede apreciar la distribución de la sucursal.

Al pedir el acceso al equipo desde el cual se habían realizado los movimientos bancarios –el equipo que estaba en servicio en la ventanilla 1 el día 2 de Abril de 2008- se encontró que este equipo no había recibido ningún tipo de

tratamiento especial para mantener la integridad de la evidencia, por el contrario este equipo había continuado en operación.

El equipo que se encontraba en operación el día 2 de Abril de 2008 tenía las siguientes características.

Tabla 5.1 Características del equipo en ventanilla.

Computadora Marca	**HP**
Modelo	VectraVL18
Número de serie	MX94450890

Mientras que el equipo que funge como servidor -el core- tiene las siguientes características.

Tabla 5.2 Características del equipo servidor.

Marca	**Compaq**
Modelo	Prosignia 200
Número de serie	D811BWP200058

2.1. Fase de Identificación Segunda Parte.

Cuando se concede el permiso de observar la recreación del sistema AS se inicia por segunda fase la fase de identificación. Ya que al observar dicha recreación se podrá tener mayor conocimiento tanto de la aplicación como de los procedimientos que se siguen en la institución bancaria.

Dicha recreación abarcará desde la iniciación, operación y baja o bloqueo del sistema; La recreación será observada por los peritos en informática involucrados en el caso y es ejecutada por dos empleados del Banco Muestra.

El primero de ellos actuará como un empleado bancario con puesto de cajero y el estará acompañado de un segundo que actuará como un empleado bancario con puesto de Subgerente de servicios.

Al iniciar el sistema se puede observar que es necesario que el subgerente de servicio haya ingresado en su equipo de cómputo al sistema, el sistema le pide su número de empleado que es de siete posiciones así como su contraseña alfanumérica que es de cuatro dígitos, esto sirve para habilitar la sucursal en el servidor central del Banco Muestra y pueda realizar operaciones; una vez hecho esto el cajero en ventanilla puede a su vez ingresar al sistema, el cual le pedirá su número de empleado y su contraseña alfanumérica de cuatro dígitos de carácter confidencial, una vez que ingresaron los datos que le pide el sistema, este le solicita al cajero que ingrese el dato de la cantidad de dinero en efectivo con lo que iniciará su caja denominado “lonchera”, que no podrá ser mayor a sesenta mil pesos, ya ingresado este dato, el sistema despliega en el monitor la pantalla para llevar a cabo operaciones propias del cajero.

En esta etapa el empleado que actúa como cajero, opera el sistema recreando operaciones de depósito en efectivo similares a las que dieron origen a la causa penal en la que se actúa, una por la cantidad de noventa y ocho mil pesos, otra por noventa y siete mil pesos, otra por cuatrocientos setenta y ocho mil pesos y la última por cuatrocientos noventa y un mil pesos, a lo que el sistema le pide que ingrese las cantidades a depositar, con las acotaciones por quienes operan el sistema, en los casos mayores a cien mil pesos, el sistema solicita la contraseña del subgerente de servicios por facultades para autorizar la operación, y el mismo sistema manda a imprimir la constancia correspondiente.

En este se aclara que si la operación la realiza directamente el subgerente de servicio por facultades, no requiere de una segunda contraseña, cosa que no sucede con el caso del cajero que forzosamente necesita de la autorización del subgerente.

En momento de la recreación la impresión de las constancias quedó en lista de espera, pero a dicho de quienes operan el sistema, indican que por lo normal inmediatamente que se ejecutan estas operaciones se imprimen, con esto da por terminada la operación.

Se continúa con la realización del bloqueo de terminal o de estación de trabajo, lo cual lo puede realizar el cajero porque el mismo sistema le da la opción, con el bloqueo de terminal se impide la realización de cualquier tipo de operación en terminal o ventanilla, mientras permanezca bloqueada.

Para desbloquear la terminal es necesario el ingreso de la contraseña confidencial o clave del cajero, esta es solicitada por el mismo sistema.

Por último en cuanto a la baja o salida temporal del sistema, este lo da como opción de pantalla, pero pide la contraseña o clave del cajero. Esta operación también fue operada por el personal actuante.

Una vez transcurrido en esta diligencia un tiempo de dos horas el personal que operó el equipo de cómputo refirió que eso era todo.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de identificación y como fue cubierta cada etapa *(Véase tabla 5.3)*.

Tabla 5.3 Etapas de la Fase de Identificación.

Fase de Identificación		
Preguntas claves	• ¿Qué partes están involucradas? • ¿Cuál es el plan de acción?	
Etapas	• Identificar el incidente.	• Fue reportado el depósito de dinero en cuentas bancarias sin registrar la entrada de ese dinero a la caja.
	• Reconocimiento de la entidad.	• Realización de cuestionarios para conocer los procesos de la entidad. • Adquisición de esquemas. • Entrevistas con personal de la entidad bancaria. • Petición de la recreación del funcionamiento de la aplicación AS.
	• Reconocimiento del personal	• Se da a conocer las personas involucradas en el incidente de seguridad.
	• Establecer un plan de acción.	• Adquisición de imágenes forenses de los equipos involucrados. • Adquisición de las cintas de grabación obtenidas por el sistema CCTV. • Elaboración de lista de palabras clave.

3. Fase de preparación.

Para el desarrollo de esta fase se cuenta con dos preguntas claves que hay que contestar:

- ¿Qué tipo de técnica se usará?
- ¿Qué se necesita?

Al contestar estas dos pregunta se identificará tanto el método o técnica que se utilizará como el equipo de hardware y software que se necesitará para poder hacer la recuperación de la evidencia que se encuentra en la escena del crimen, o bien que se encuentra involucrada.

La elección del equipo que se utilizará se hace derivada de la información que se recabó en la fase de Identificación.

En este caso como sabemos que la información se encuentra almacenada en discos duros de dos computadoras lo más conveniente es la realización de imágenes de estos discos.

Al obtener la imagen de los discos se asegura la obtención de toda la información almacenada en los ellos. Si algún tipo de información trato de ser eliminada por métodos comunes se podrá encontrar el registro de estos y probablemente se podrá recuperar la información.

Una vez que se ha elegido la técnica por la cual se hará la adquisición de la evidencias entonces se podrá hacer la elección tanto del software –herramientas, sistemas operativos, programas…- como del equipo hardware que se requerirá.

Se decidió usar el sistema operativo Backtrack Final Release versión 4 ya que es un sistema operativo que cuenta con adaptaciones especiales para realizar análisis forense.

Además se acordó que se usará el live CD de este sistema operativo para evitar que se registren cambios en la información contenida en los discos de la entidad bancaria.

Para el equipo de hardware se optó por la utilización de un equipo de cómputo portátil para poder trasladarlo hasta el lugar donde se encontrara la evidencia.

A continuación se muestra una lista del equipo y de las herramientas seleccionadas para hacer la adquisición de evidencia.

1. Equipo de cómputo portátil, procesador Intel Centrino Core 2 Duo corriendo a 2.4 GHz y memoria RAM total de 4GB.

2. Sistema operativo adaptado especialmente para análisis forense, corriendo en memoria RAM y arrancado desde un Live CD. El sistema operativo estará basado en una distribución Linux Ubuntu, cuyo nombre es Backtrack Final Release versión 4, sistema operativo libre y público.

3. Herramienta “dd” herramienta nativa en la familia de sistemas operativos basados en UNIX, cuyo fin es crear una copia bit a bit del dispositivo y almacenar los datos en un archivo digital para su análisis.

4. herramientas md5summer y md5deep para obtener las huellas digitales de los discos y garantizar que las copias obtenidas con la herramienta “dd” correspondieran inequívocamente a los dispositivos de almacenamiento que se analizaron.

   El equipo de cómputo seleccionado para hacer la adquisición de la evidencia tuvo un tratamiento previo para asegurar que contaba con espacio suficiente para almacenar la evidencia y verificar que el disco que

se va a utilizar se encuentra limpio, es decir que no cuenta con ningún tipo de información.

Además se instaló en el equipo de cómputo las herramientas necesarias para poder realizar la adquisición de la evidencia. En este caso se instaló la herramienta md5summer.

En el caso de la herramienta dd no fue necesario instalarla ya que viene como una herramienta nativa del sistema operativo Backtrack Final Release.

Por último se previó contar con los cables necesarios para poder conectar cualquier tipo de disco duro que poseyera el equipo de cómputo de la entidad bancaria.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de preparación y como fue cubierta cada etapa *(Véase tabla 5.4)*

Tabla 5.4 Etapas de la Fase de Preparación.

Fase de Preparación		
Preguntas claves	• ¿Qué tipo de técnica se usará? ¿Qué se necesita?	
Etapas	• Identificación del equipo hardware.	• Equipo de cómputo portátil, procesador Intel Centrino Core 2 Duo corriendo a 2.4 GHZ y memoria RAM de 4GB.
	• Identificación del equipo software	• Sistema operativo Backtrack Final Release versión 4 • Herramienta “dd” • Herramienta md5summer
	• Preparación del equipo.	• Contar con el espacio necesario para guardar la evidencia del caso. • Contar con la instalación de herramientas que garanticen la integridad de la evidencia. • Contar con cables para realizar las imágenes forenses.

4. Fase de adquisición de evidencia.

En esta fase se contestará la pregunta ¿Cómo adquirir la evidencia? Al contestar esta pregunta obtendremos el orden en el que se hará la adquisición de la evidencia y el método por el cual se hará.

Antes de pensar en realizar la adquisición de evidencia se debe de tener el permiso de la entidad para poder hacerlo de lo contrario se estaría cayendo en un delito.

Por lo cual para hacer la adquisición de evidencia de la entidad bancaria antes se solicitó el permiso pertinente para poder tener acceso a los equipos de cómputo y de realizar las imágenes forenses necesarias para hacer el análisis. Así como de videograbar y fotografiar las instalaciones y posiciones de las cámaras de seguridad con las que cuenta la institución.

Como segunda petición el perito en informática solicitó el código fuente y ejecutable de las aplicaciones tanto del servidor –core- como del cliente y de todo código necesario para realizar el análisis de la funcionalidad y seguridad del sistema.

Por último se solicitaron los videos correspondientes a las grabaciones de las cámaras de CCTV el día 2 de abril de 2008.

La entidad bancaria aceptó que el perito realizara la visita a las instalaciones donde se localizaba la aplicación cliente, la aplicación servidor y el acceso al equipo de cómputo involucrado en el caso.

Se concedió el permiso de verificar la posición de las cámaras del circuito cerrado (CCTV) y la operación de las mismas. Solicitando que la visita se realizara en días y horas hábiles.

En el caso de la solicitud de códigos fuente y ejecutables la institución bancaria contestó que no le era posible proporcionarlos debido a que dichos códigos y ejecutables permanecen en uso constante y son necesarios para sustentar la operación y los procesos del banco.

Y con respecto a la solicitud de las grabaciones de las cámaras, la entidad bancaria contestó que el equipo que concentraba la información de los archivos presentó fallas electrónicas que daño los archivos por lo que se declaraban imposibilitados para exhibir los videos requeridos.

Esto dejó sólo la posibilidad de adquirir la evidencia que se encontrara en los discos duros de los equipos de la entidad. Al encontrarse la evidencia en discos duros ambas tienen el mismo tiempo de volatilidad, así que para determinar cual tendría prioridad en el momento de la adquisición se tendría que tomar en cuenta el estado en el que se encuentra cada uno de los discos –en funcionamiento o apagado-.

¿Cómo se encontraban los discos duros en el momento de hacer la adquisición de la evidencia?

¿De qué tamaño eran los discos o cómo fue que sólo se pudieron obtener dos imágenes de esos tamaños? Esto va en la fase de identificación.

Una vez que se determinó el orden en el que se realizaría la adquisición de la evidencia y el tamaño de ésta, se decidió el método por el cual se realizarían las imágenes forenses.

La herramienta que se utilizaría para la adquisición de la evidencia ya se había preparado seria la herramienta “dd” sin embargo la elección del método se tomaría hasta conocer el estado y tamaño de la evidencia de la cual se sacarían las imágenes forenses.

En este caso como las imágenes forenses serian de un máximo de 5GB no fue necesario utilizar un método de adquisición que nos seccionara la evidencia en pequeños archivos ya que poseíamos el espacio suficiente para almacenar la evidencia proporcionada por la entidad.

Por lo que el método que se eligió para adquirir la imagen forense fue la copia bit a bit de disco a archivo.

Para hacer la adquisición de evidencia se usó el equipo de cómputo que se dispuso en la fase de preparación –equipo portátil con procesador Intel Centrino Core 2 Duo corriendo a 2.4 GHZ y memoria RAM de 4GB-

El sistema operativo Backtrack se arrancó desde un Live CD para evitar que se registraran cambios en la evidencia.

La imagen se obtuvo usando la herramienta "dd" herramienta que se encuentra de forma nativa en la familia de los sistemas operativos basados en UNIX. Esta herramienta creo la copia bit a bit del dispositivo y almacenó los datos en un archivo digital para su posterior análisis.

Los resultados que se obtuvieron de dicho proceso fueron los siguientes *(Véase tabla 5.5, 5.6 y 5.7)*.

Tabla 5.5 Herramienta para la adquisición de imágenes forenses.

Herramienta para adquisición de imagen de Disco Duro.	
Sistema Operativo	Backtrack 4 Final Release
Huella digital oficial	af139d2a085978618dc53cabc67b9269
Sitio oficial del sistema	http://www.backtrack-linux.org/downloads/
Huella digital obtenida	af139d2a085978618dc53cabc67b9269

Tabla 5.6 Nombre y tamaño de la imagen forense ventanilla 1.

Disco Duro 1 (Ventanilla1)	
Nombre de la imagen	imgV1MR.img
Tamaño	4.01GB

Tabla 5.7 Nombre y tamaño de la imagen forense del servidor.

Disco Duro 2 (Servidor)	
Nombre de la imagen	imgSevMR.im
Tamaño	4.24GB

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de adquisición de evidencia y como fue cubierta cada etapa *(Véase tabla 5.8)*.

Tabla 5.8 Etapas de la Fase de Adquisición de evidencia.

Fase de Adquisición de evidencia		
Preguntas claves	¿Cómo adquirir la evidencia?	
Etapas	• Identificación de métodos apropiados	• Uso del método bit a bit a archivo para realizar la adquisición de evidencia.
	• Establecimiento del orden de prioridad	• Verificación del tipo de dispositivo en donde encuentra almacenada la evidencia • El estado en el que se encuentra el dispositivo
	• Autoridad legal	• Se solicitaron los permisos necesarios para poder adquirir la evidencia
	• Toma de muestras	• Se sacaron dos imágenes forenses una del equipo de ventanilla y la otra del equipo del servidor.

5. Fase de preservación.

En esta fase se busca la respuesta a la pregunta ¿Cómo preservar la evidencia?

Para poder preservar la evidencia obtenida lo primero que se tiene que realizar es la comprobación de que los datos que contiene la imagen forense obtenida correspondan exactamente con los datos contenidos en el los discos duros que pertenecen a la entidad bancaria.

La comprobación de que los datos de la imagen forense correspondían a los almacenados en los discos duros se realizó mediante el empleo de una función hash. La cual nos entrega una cadena de caracteres que identifica unívocamente a un conjunto de datos.

En este caso se empleó la herramienta md5summer y md5deep para obtener las huellas digitales de los discos y comprobar que estas correspondan con las huellas obtenidas de las imágenes forenses.

Esta herramienta utiliza el algoritmo md5, el cual regresa como resultado una cadena de 32 caracteres para identificar un archivo.

Los resultados obtenidos después de este procedimiento fueron los que se presentan en las siguientes tablas *(Véase tablas 5.9 y 5.10).*

Tabla 5.9 Valor hash de la imagen forense de la ventanilla1.

Disco Duro 1 (Ventanilla1)	
Huella digital original de disco	439140790a83dd7109f1629d92ab6976
Huella digital de imagen obtenida	439140790a83dd7109f1629d92ab6976

Tabla 5.10 Valor hash de la imagen forense del servidor.

Disco Duro 2 (Servidor)	
Huella digital original de disco	4d5dac2ca56da415f4ab540a25eac4f3
Huella digital de imagen obtenida	4d5dac2ca56da415f4ab540a25eac4f3

Para garantizar la preservación de los datos adquiridos se tomaron las siguientes medidas.

Una vez que se obtuvieron las imágenes forenses estas fueron etiquetadas para que no fueran confundidas durante el traslado desde la entidad bancaria hasta el laboratorio de seguridad informática, en donde serian analizadas.

Después de etiquetar las imágenes forenses se inicia la cadena de custodia de estas imágenes para garantizar que estas se conserven integras hasta llegar al laboratorio. En esta cadena de custodia se nombra a un responsable, se describe el dispositivo contenedor de la evidencia y se registra su huella o resultado de la función hash.

En cuanto la evidencia llegó al laboratorio de seguridad informático, se hicieron copias de respaldo de las imágenes forenses con el objetivo de mantener la integridad de los datos. De esta manera se guardarían las copias obtenidas en el lugar del incidente en un lugar seguro con acceso restringido y las copias obtenidas en el laboratorio se utilizarían para hacer el análisis forense.

Al realizar este procedimiento –sacar copias de respaldo- se marcó la copia obtenida en la entidad bancaria como “Limpia” y la obtenida en el laboratorio de seguridad como “Trabajo”.

Se comprobó que las huellas de los respaldos – las copias etiquetadas como “Trabajo”- coincidieran con las copias obtenidas en el lugar del incidente – copias etiquetadas como “Limpia”.

Para poder comparar las dos imágenes forenses –las obtenidas en el laboratorio contra las obtenidas en la entidad bancaria- se calculó la función hash de las copias obtenidas en el laboratorio para lo cual se utilizaron las herramientas md5summer y md5deep.

A continuación se muestra una tabla con las preguntas claves y las etapas correspondientes a esta fase de preservación y como fue cubierta cada etapa *(Véase tabla 5.11).*

Tabla 5.11 Etapas de la Fase de Preservación.

Fase de Preservación		
Preguntas claves	¿Cómo conservar la evidencia?	
Etapas	• Métodos de traslado	• Etiquetado de la evidencia para su traslado.
	• Seguimiento de la cadena de custodia.	• Uso de funciones hash que garanticen la integridad de la evidencia. • Se inician los formatos para la cadena de custodia.
	• Respaldos	• Se realizaron dos copias de respaldo. • Almacenamiento de la evidencia en un lugar seguro.

6. Fase de análisis.

La pregunta clave de esta fase es: ¿Es un dato clave? Esta fase se dividirá en tres partes: preparación, análisis y recuperación.

En la fase de preparación se harán las actividades necesarias para lograr tener el equipo necesario para analizar la evidencia obtenida previamente.

6.1 Preparación

Para la realización del análisis de las imágenes se destinaron tres máquinas distintas, esto con la finalidad de tener un abanico amplio en cuanto a las herramientas que se pueden utilizar y poder verificar los resultados obtenidos.

A continuación se da la descripción de cada una de las computadoras destinadas para el análisis *(Véase tabla 5.12, 5.13 y 5.14)*.

Tabla 5.12 Características de la Máquina Windows.

Máquina 1 Windows	
Procesador	Intel Core i3 corriendo a 3.07 GHz
Memoria RAM	4GB
Sistema Operativo	Windows 7 Ultimate SP1 a 64 bits

Tabla 5.13 Características de la Máquina Linux.

Máquina 2 Linux	
Procesador	Intel Core2 Duo a 1.5 GHz
Memoria RAM	2GB
Sistema Operativo	Linux Ubuntu a 64 bits

Tabla 5.14 Características de la Máquina Mac.

Máquina 3 MAC	
Procesador	Intel Core2 Duo a 2.16 GHz
Memoria RAM	1GB
Sistema Operativo	Mac OS x versión 10.6.3

Para cuidar la integridad de la evidencia, se conectaran los dispositivos que contienen la evidencia en modo de solo lectura para evitar que se produzca algún cambio en ellos.

6.2. Análisis.

En esta fase se someterá la evidencia adquirida a diferentes tipos de análisis buscando las pruebas necesarias que ayuden a aclarar el caso. En esta fase será muy útil la lista de palabras claves que se ha estado realizando en las fases encontradas, pues reducirá el volumen de la información que tenga que ser analizada.

A continuación se mostraran los pasos seguidos durante esta fase. Algunos de los resultados obtenidos no podrán ser mostrados ya que se pondría en peligro el acuerdo de confidencialidad. Sin embargo será descrito cada uno de los resultados y el procedimiento que se siguió para obtenerlos.

6.2.1 Verificación de Integridad

El cuidar la integridad de la evidencia es una actividad que se tiene que realizar durante toda la investigación. En gran parte la veracidad de las pruebas presentadas residirá en la prueba de su integridad.

Lo primero que se verificó al conectar el dispositivo contenedor de evidencia fue que este no hubiera sufrido cambios. Para comprobar su integridad se calculó su función hash y se comparó con la huella calculada en el momento de la adquisición de evidencia hecha en el banco.

A continuación se muestran las capturas de pantalla tomadas en el momento de acceder a la evidencia por medio de la herramienta Autopsy Sleuth Kit, herramienta con la cual se pudo verificar la integridad de la evidencia ya que

cuenta con opciones para calcular la función hash de las imágenes forense. El algoritmo utilizado fue MD5.

En la figura 5.2 que se presenta a continuación, se puede ver el nombre de la imagen en este caso imgV1MR.img y su correspondiente hash 439140790a83dd7109f1629d92ab6976.

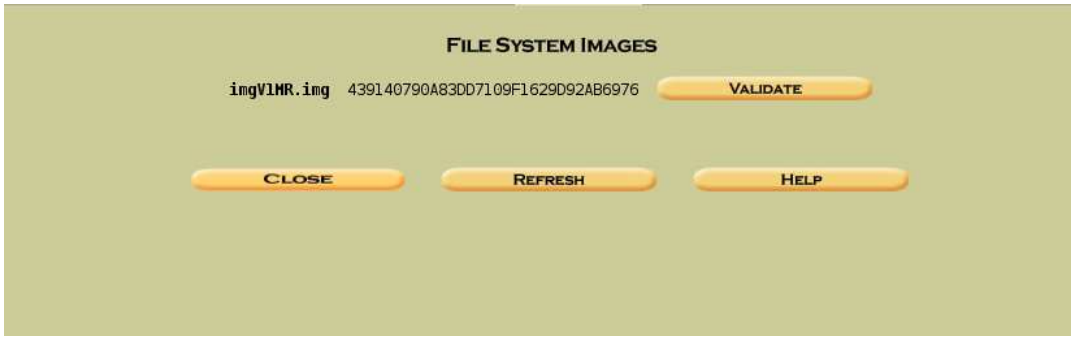


Figura 5.2 Imagen que muestra el valor hash de la imagen forense capturada del equipo de la ventanilla1.

Autopsy Sleuth Kit es una de las herramientas utilizadas para el análisis de la evidencia. Esta herramienta permite examinar el sistema de archivos de una computadora sin comprometerla -sin dañar su integridad-.

Debido a que esta herramienta no procesa el sistema de archivos con ayuda del sistema operativo puede mostrarnos el contenido de archivos borrados u ocultos.

Al comparar este valor con el que se calculó en el momento de hacer la adquisición, se obtienen los resultados de la siguiente tabla *(Véase tabla 5.15).*

Tabla 5.15 Comparación de los valores hash (ventanilla1).

Disco Duro 1 (ventanilla1)	
Hash del la imagen en el momento de la adquisición.	439140790a83dd7109f1629d92ab6976
Hash de la imagen en el momento de empezar el análisis.	439140790a83dd7109f1629d92ab6976

Como se puede ver los dos valores hash coinciden esto quiere decir que la imagen no ha sufrido ningún tipo de alteración en los datos –se conserva integra-. Una vez seguros de esto podemos confiar en que los resultados serán confiables y validos ante una corte judicial.

La siguiente imagen corresponde a la captura de pantalla tomada en el momento de acceder a la imagen correspondiente al disco duro 2 que corresponde al servidor de la entidad bancaria *(Véase fig. 5.3)*

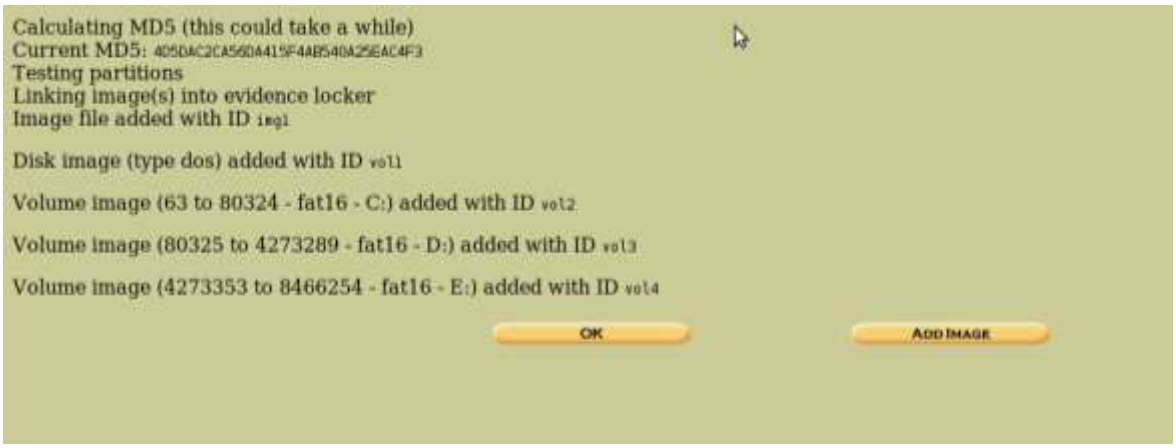


Figura 5.3. Imagen que muestra el valor hash de la imagen capturada del servidor.

Se puede observar en esta imagen el cálculo del valor hash utilizando el algoritmo MD5. En ese caso el valor es: 4d5dac2ca56da415f4ab540a25eac4f3

Al obtener el valor hash de la imagen se compara con el valor obtenido en el momento de la captura de la evidencia. El resultado es el siguiente *(Véase tabla 5.16)*.

Tabla 5.16 Comparación de los valores hash (servidor).

Disco Duro 2 (servidor)	
Hash del la imagen en el momento de la adquisición.	4d5dac2ca56da415f4ab540a25eac4f3
Hash de la imagen en el momento de empezar el análisis.	4d5dac2ca56da415f4ab540a25eac4f3

La verificación del valor hash de las imágenes se hizo siempre que se conectó el dispositivo contenedor de la evidencia en cualquiera de las máquinas destinadas para la realización del análisis.

Una vez que se verificó que la imagen se encontrara integra se realizó la identificación de los sistemas operativos y especificaciones de cada una de las imágenes.

6.2.2 Identificación de los sistemas.

Identificar el tipo de sistemas operativos y sistemas de archivos utilizados por cada una de las imágenes forenses obtenidas es muy importante, pues al conocer estos datos conoceremos como es su funcionamiento y el tipo de organización de archivos que tiene.

De esta manera será más sencillo para el analista forense intuir en que carpetas buscar la evidencia que necesita, esta evidencia puede ser bitácoras, información del usuario, programas instalados, registro de IP conectadas en dicha máquina, etc.

A continuación se mostraran los resultados que se obtuvieron al montar las imágenes en la máquina uno que opera con el sistema operativo Windows.

Para montar las imágenes en la máquina 1 Windows se utilizó un programa llamado Mount Image Pro v4.

La siguiente imagen muestra la captura de pantalla tomada al momento de montar la imagen forense correspondiente a la “ventanilla1” con la herramienta Mount Image Pro v4 *(Véase fig. 5.4)*.

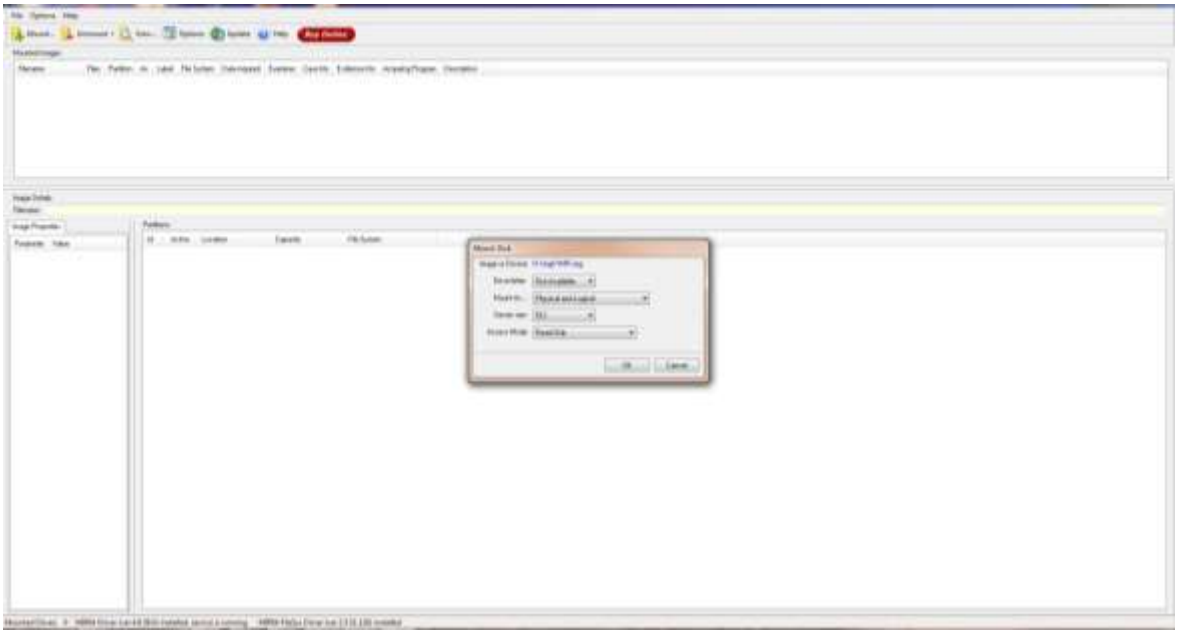


Figura 5.4. Captura de pantalla al momento de montar la imagen forense de la ventanilla1 con la herramienta Mount Image Pro v4.

En esta imagen se puede observar que al ser montada la imagen se especifica que el acceso a ella sea de sólo lectura. Esto se hace para cuidar la integridad de la evidencia durante el análisis.

Al ser montada la imagen la herramienta nos muestra las características de la imagen como son su capacidad, número de sectores y sistema de archivos entre otros *(Véase fig. 5.5)*.

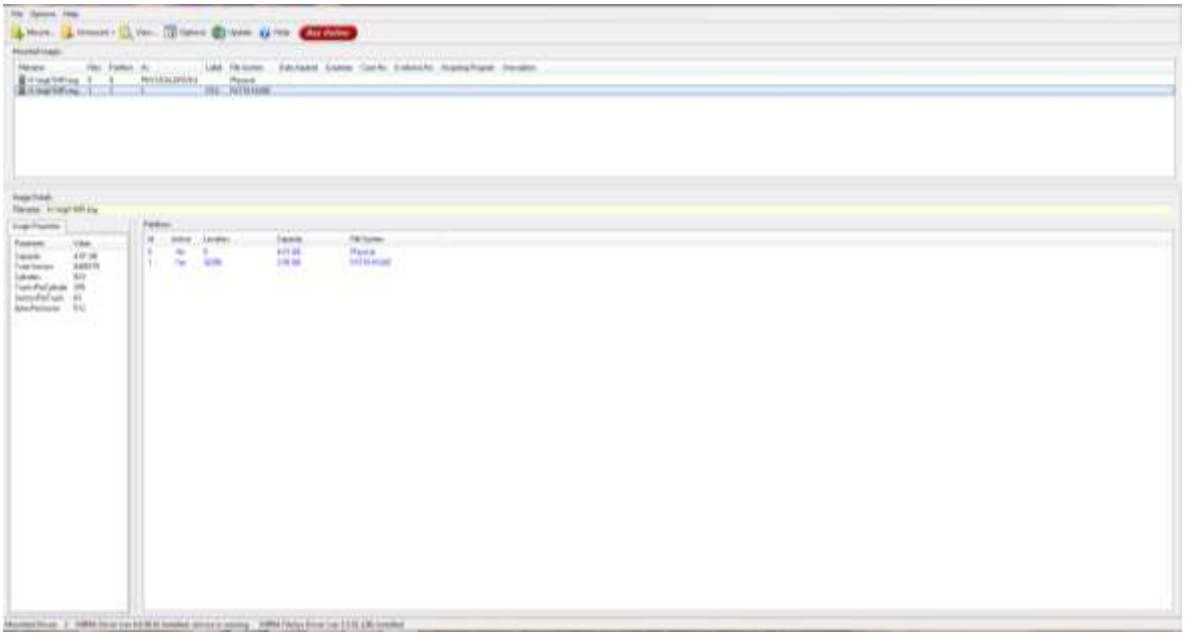


Figura 5.5. *Características de la imagen correspondiente a la Ventanilla1 mostradas por la herramienta Mount Image Pro v4.*

Las características que nos muestra esta herramienta se listan en la siguiente tabla *(Véase tabla 5.17).*

Tabla 5.17 Características de la imagen forense de la ventanilla1 mostradas por la herramienta Mount Image Pro v4.

Capacidad	**4.01GB**
Total de sectores	8405775
Cilindros	523
Numero de particiones	1
Localización de la partición	32256
Capacidad de la partición	2.00GB
Tipo de sistema de archivos	FAT16 HUGE

Al consultar las propiedades de la imagen desde el sistema Windows obtenemos la siguiente información *(Véase tabla 5.18 Y fig.5.6)*.

Tabla 5.18 Características de la imagen forense de la ventanilla1 mostradas por el sistema Windows.

Sistema de Archivos	FAT
Sistema Operativo	OS/2 de IBM[23]
Capacidad	2144043008 bytes (1.99GB)
Espacio usado	615 MB
Espacio disponible	1.39 GB

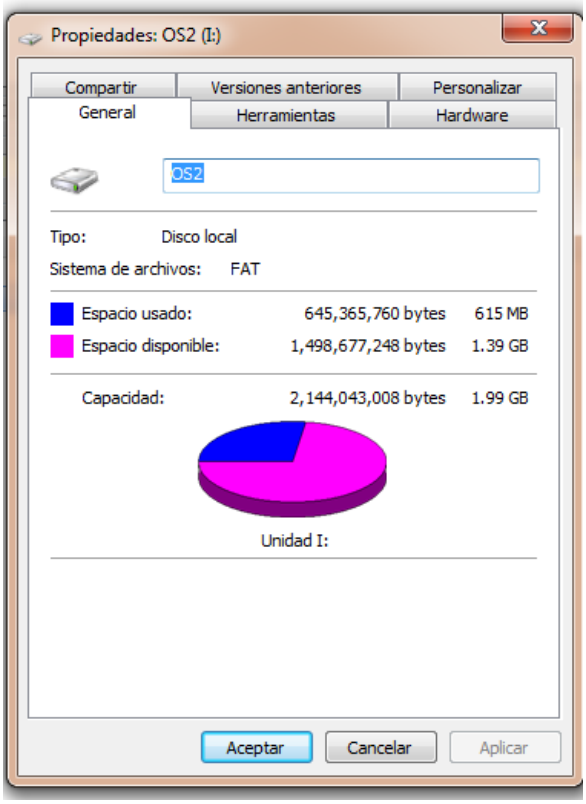


Figura 5.6 Características de la imagen forense de la ventanilla1 mostradas por el sistema Windows.

[23] Sistema Operativo creado por Microsoft e IBM "Operating System/2" buscaba remplazar a MS-DOS sin embargo Microsoft decidió continuar con Windows 3.0 e IBM se ocupo de OS/2. La versión 1.0 salió en 1987 y su última actualización fue en abril del 2002. A finales de 2005 IBM retiró OS/2 del mercado.

De esta manera obtuvimos que en la imagen “Ventanilla1” se utiliza un sistema operativo OS/2 con un sistema de archivos FAT 16 HUGE.

El sistema operativo OS/2 es un sistema operativo desarrollado por IBM. Este sistema operativo se crea como sucesor del sistema DOS para PC e intenta direccionar los nuevos requerimientos de una industria madura de PC.

Este sistema operativo puede utilizar sistemas de archivos FAT o HPFS, este último sistema de archivos fue diseñado especialmente para los sistemas OS/2, ofrece nombres de archivos largos, incluye metadatos e información de seguridad y mejor velocidad en relación al FAT.

Este sistema operativo proporciona una interfaz gráfica de ventanas similar a la de Windows 95.

Continuando con la identificación de los sistemas se realizó el mismo procedimiento ahora con la imagen “servidor”.

De la misma manera que se cuidó que el acceso fuera de sólo lectura con la imagen “ventanilla 1” también se hizo con la imagen “servidor”.

A continuación se muestra la captura de pantalla al momento de montar la imagen forense “ventanilla 1” con la herramienta Mount Image Pro v4 *(Véase fig. 5.7).*

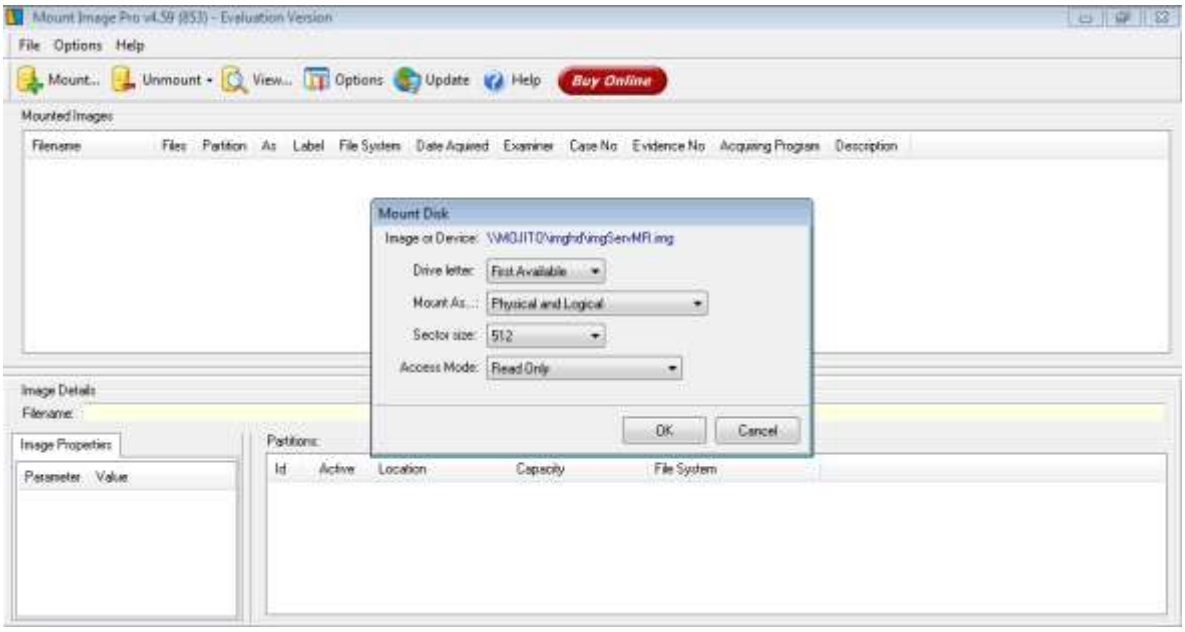


Figura 5.7. *Captura de pantalla al momento de montar la imagen forense del servidor con la herramienta Mount Image Pro v4.*

Una vez montada la imagen se puede ver con cuantas particiones cuenta, cual es el formato que tiene cada una de ellas, así como el tamaño que tiene y como está distribuido *(Véase fig. 5.8)*.

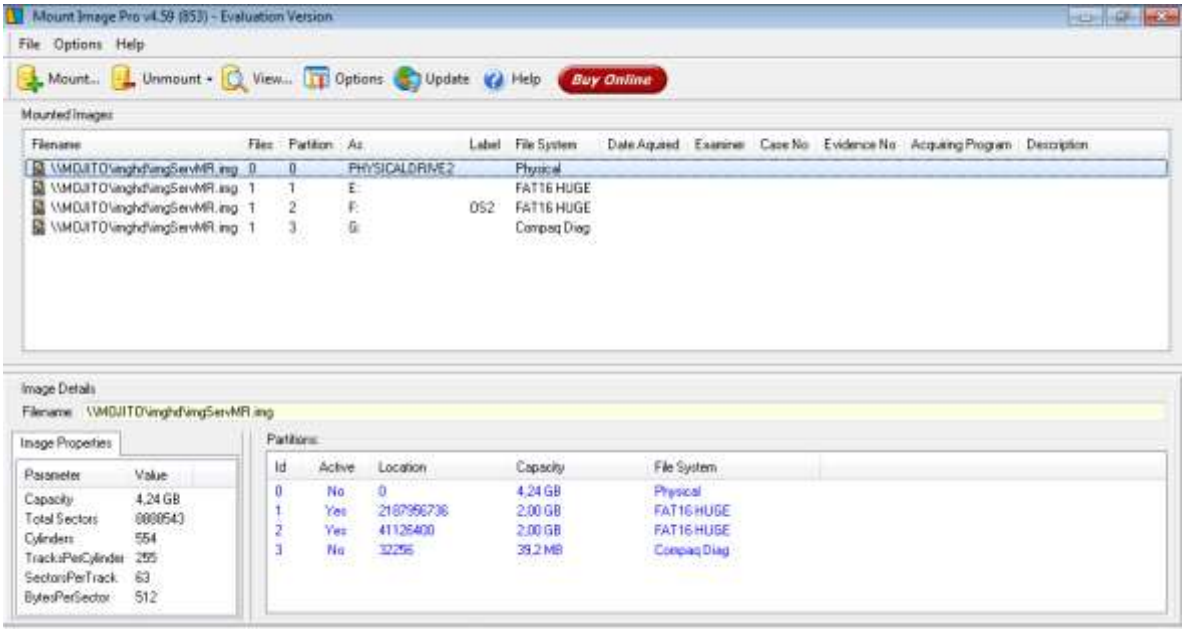


Figura 5.8. *Características de la imagen correspondiente al servidor mostradas por la herramienta Mount Image Pro v4.*

En la tabla 5.19 se enlistan las características de la imagen forense correspondiente al servidor arrogadas por la herramienta Mount Image Pro v4.

Tabla 5.19 Características de la imagen forense correspondiente al servidor.

Capacidad	**4.24GB**
Total de sectores	8888543
Cilindros	554
Numero de particiones	3
Localización de la partición 1	2187956736
Capacidad de la partición 1	2.00GB
Tipo de sistema de archivos de la partición 1	FAT16 HUGE
Localización de la partición 2	41126400
Capacidad de la partición 2	2.00GB
Tipo de sistema de archivos de la partición 2	FAT 16 HUGE
Localización de la partición 3	32256
Capacidad de la partición 3	39.2MB
Tipo de sistema de archivos de la partición 3	Compaq Diag

Si abrimos la información que nos da Windows acerca de cada partición podemos ver el espacio usado, el espacio disponible y la capacidad de cada una de las particiones.

A continuación se muestra la información adquirida de cada una de las particiones. Se puede ver que Windows les ha asignado una letra a cada partición para nombrarlas la cual no corresponderá a la que tenía en la máquina original.

En este caso las letras que les asignó el sistema Windows fueron las letras E, F y G.

En las siguientes tablas y figuras se pueden ver las características obtenidas de cada una de las tres particiones encontradas en la imagen forense del servidor *(Véase tabla 5.20, 5.21 y 5.22 y las fig. 5.9, 5.10 y 5.11).*

Tabla 5.20 Características de la partición uno encontrada en la imagen forense del servidor.

Sistema de Archivos	FAT
Capacidad	2146467840 bytes (1.99GB)
Espacio usado	1.08 GB
Espacio disponible	935 MB

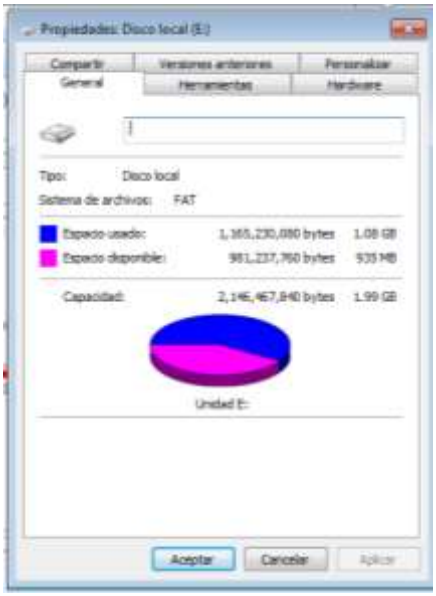


Figura 5.9. Información de la partición uno vistas desde Windows.

La siguiente tabla e imagen muestra la información de la partición dos encontrada en la imagen forense correspondiente al servidor *(Véase tabla 5.21 y fig. 5.9)*.

Tabla 5.21 Características de la partición dos encontrada en la imagen forense del servidor.

Sistema de Archivos	FAT
Capacidad	2146500608 bytes (1.99GB)
Espacio usado	1.00 GB
Espacio disponible	.99 GB

Figura 5.10 Información de la partición dos vista desde Windows.

La siguiente tabla e imagen muestra la información de la partición tres encontrada en la imagen forense correspondiente al servidor *(Véase tabla 5.22 y fig. 5.11)*.

Tabla 5.22 Características de la partición tres encontrada en la imagen forense del servidor.

Sistema de Archivos	FAT
Capacidad	40994816 bytes (39MB)
Espacio usado	12 MB
Espacio disponible	27 MB

Figura 5.11 Información de la partición tres vista desde Windows.

Una vez que se conoce el tipo de partición que vamos a sujetar a análisis entonces seleccionamos las herramientas que nos ayudarán a realizar este trabajo. En este caso en la máquina de Windows usamos la herramienta llamada FTK Imager (Forensic ToolKit).

FTK Imagen es una herramienta de cómputo forense que nos permite crear imágenes, analizar el registro, conducir una investigación descifrar archivos, romper contraseñas e identificar archivos con esteganografía.

Usando la herramienta FTK podemos acceder a la imagen forense, La cual nos mostrará del lado izquierdo una sección en donde veremos el árbol de evidencia[24], de lado derecho en la parte superior la herramienta nos mostrara los archivos que contiene la carpeta seleccionada y en la parte inferior tendremos el archivo abierto, el cual lo podemos ver en dos diferentes formas: En un formato de texto plano o en un formato hexadecimal.

En la computadora en la cual usamos Ubuntu Linux usaremos una herramienta llamada The Sleuth Kit (TSK). Esta es una librería que contiene una colección de comandos en línea que permiten investigar volúmenes o particiones y datos en los diferentes sistemas de archivos.

La herramienta que permite examinar el sistema de archivos tiene la ventaja de ser una herramienta no intrusiva. Debido a que no se basa en el sistema operativo para procesar los archivos puede mostrar los archivos borrados y ocultos.

Cuenta con una interfaz gráfica llamada Autopsy Sleuth Kit la cual es accedida desde un navegador para proporcionar una interfaz más cómoda al usuario.

La herramienta funciona en sistemas Linux, OS X, FreeBSD, OpenBSD y Solaris y puede analizar formatos FAT, NTFS, UFS, EXT2FS y EXT3FS.

En la interfaz gráfica de esta herramienta podemos ver del lado izquierdo un árbol con todos los archivos que contiene la partición, de lado derecho encontramos un menú que contiene: Análisis de archivos, Búsqueda de palabras clave, Tipo de archivos, Detalles de la Imagen, Metadatos, Datos de la unidad, Ayuda y Cerrar.

[24] Un listado de todos los archivos que contiene la imagen organizado en carpetas y subcarpetas

En la parte inferior derecha podemos ver los archivos que contiene la carpeta selecciona y algunos detalles de éstos, al ser seleccionados en la parte de abajo se muestra su contenido en ASCII o Hexadecimal. Los archivos pueden ser exportados o se les puede adjuntar una nota.

Lo primero que haremos al abrir la imagen es analizar los primeros 512 bytes en los cuales se encuentra el tipo de sistema operativo y sistema de archivos es el que usa.

A continuación se mostrara el análisis realizado a estos 512 bytes. Se mostraran los resultados obtenidos con la herramienta FTK aunque de igual forma se pueden obtener estos resultados usando la herramienta Autopsy Sleuth Kit.

En la herramienta FTK si se quiere analizar los primeros 512 bytes de la imagen forense con la finalidad de conocer el tipo de sistema operativo que contiene, es necesario acceder a la imagen forense de modo hexadecimal.

De esta manera la herramienta nos mostrará cada uno de los valores contenidos en los sectores que conforman la imagen forense

Conocer el tipo de sistema operativo que tiene la imagen forense es indispensable ya que dependiendo de este será el sistema de archivos que utilice. Y una vez conociendo el sistema de archivos utilizado se podrá conocer la organización de los archivos y la ubicación de cierta información.

En la siguiente captura de pantalla podemos ver la información de los primeros 512 sectores en formato hexadecimal de la imagen forense correspondiente a la ventanilla 1 *(Véase fig*.5.12).

Figura 5.12 Primeros 512 bytes de la imagen forense correspondiente a la ventanilla1.

De esta manera comprobamos que efectivamente el sistema operativo que se utiliza es el OS/2. Esta información se puede encontrar en la cadena hexadecimal 4F532F32, y el sistema de archivos que usa es FAT 16.

6.2.3 Análisis de archivos.

Dentro del análisis de archivos se incluyó:

- La realización del listado de archivos.
- Detección de archivos ocultos y borrados.
- Detección de archivos utilizando algún sistema de cifrado.
- Búsqueda de bitácoras generadas por el sistema AS.
- Verificación de establecimiento de conexiones.
- Análisis de los tiempos para realizar las transacciones.

- Análisis de las cintas imágenes capturadas por el sistema de Circuito Cerrado de Televisión –CCTV-.
- Información sobre la red.
- Verificación de programas instalados.

Para realizar el análisis de los archivos se usaron las herramientas FTK imager –en la estación de análisis que tiene Windows- y Sleuth Kit Autopsy –en la estación de trabajo que usa Linux-

6.2.3.1 Listado de archivos y detección de archivos ocultos o borrados.

Para poder realizar el listado de archivos se abrieron las imágenes forenses con las herramientas FTK imager y Sleuth Kit Autopsy.

Al cargar la imagen forense con la herramienta FTK imager, se tiene acceso a los archivos que contiene esta imagen tanto a los que se encuentran en un espacio asignado como las que se encuentran en espacios no asignados –archivos que han sido borrados- *(Véase fig. 5.13)*.

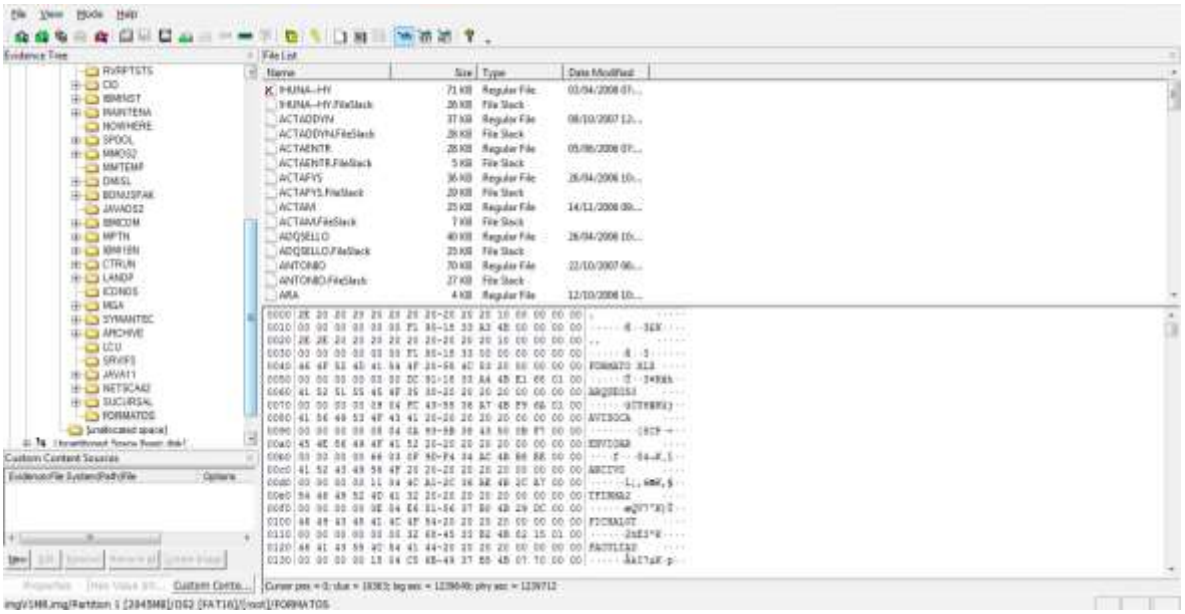


Figura 5.13 Imagen forense abierta con la herramienta FTK Imager.

En la figura 5.13 Se puede apreciar el árbol de archivos que se muestra en la parte izquierda de la figura, en donde podemos navegar por los diferentes directorios que contiene la imagen forense. Del lado derecho en la parte superior podemos ver el contenido del directorio que hayamos seleccionado y en la parte inferior podemos ver los datos contenidos en el archivo que se haya seleccionado.

El contenido de un archivo se puede ver de tres formas diferentes: abriéndolo automáticamente en un archivo de texto o en un navegador de internet, viéndolo en texto plano y viendo el archivo en un formato hexadecimal.

Los archivos que hayan sido eliminados se podrán visualizar marcados con una tache de color rojo sobre el icono que marca que se trata de un archivo. En la figura 5.14 Se puede ver que el primer archivo que se despliega es un archivo que ha sido eliminado. Sin embargo se puede tener acceso a su contenido y extraerlo en caso de tenerlo como un archivo de texto.

Al trabajar en la estación de análisis cargada con Linux accederemos a las imágenes forenses por medio de la interfaz gráfica digital de la herramienta Sleuth Kit Autopsy.

Cuando se accede a los archivos contenidos en la imagen forense se puede tener acceso a los archivos eliminados u ocultos, se puede tener acceso a ellos navegando por los directorios o bien seleccionando el sector del disco al cual se desea acceder.

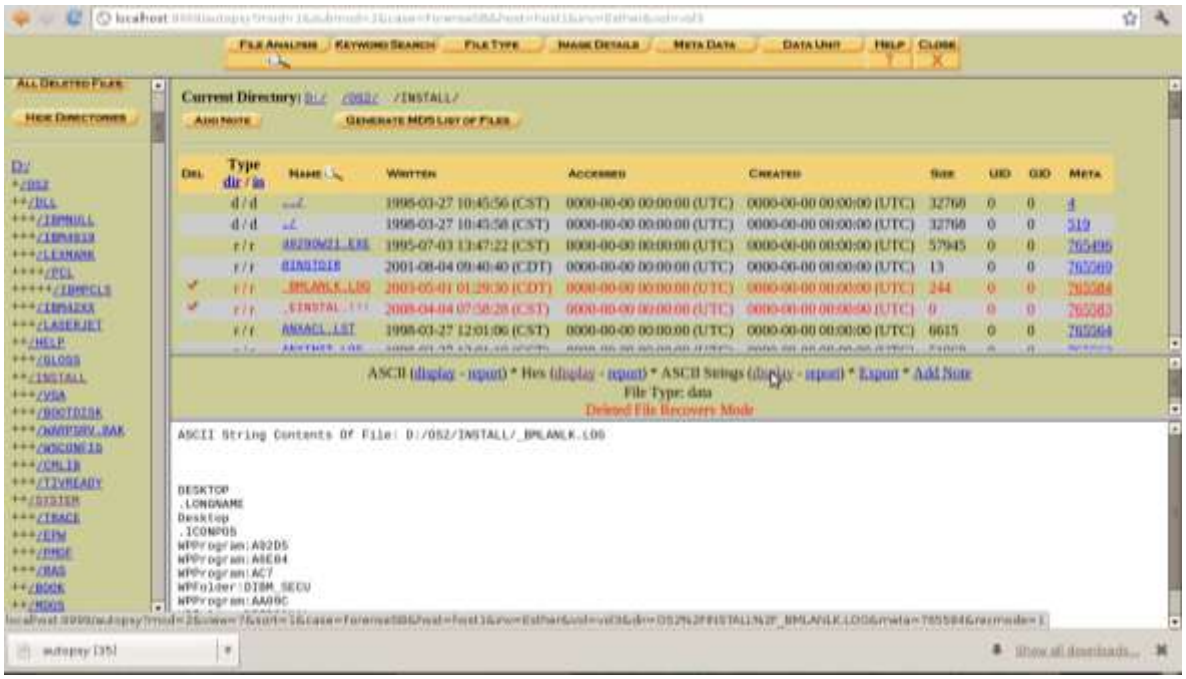


Figura 5.14 Imagen forense abierta con la herramienta Sleuth Kit Autopsy.

En la figura 5.14 ,que muestra la pantalla que se observa al acceder a la imagen forense por medio de la herramienta Sleuth Kit Autopsy, se puede ver que esta herramienta muestra del lado izquierdo el listado de todos los directorios que contiene la imagen forense, estos se encuentran organizados en directorios y subdirectorios.

Del lado derecho se puede tener acceso a los archivos que contiene el directorio que se haya seleccionado, y en la parte inferior se podrá ver el contenido de ese archivo el cual se puede acceder de tres formas distintas: en un formato hexadecimal, en un formato de texto plano visto en la misma aplicación o en un formato de texto plano extraído y abierto con algún editor de texto.

Esta herramienta, marca de color rojo los archivos que se encuentran en un espacio no asignado –archivos que han sido eliminados- y con azul los archivos que se encuentran en espacios asignados.

Desde esta herramienta es fácil acceder a información como los metadatos o los detalles de la imagen, en donde podemos encontrar información como el

nombre del volumen, el sistema de archivos utilizados, la distribución de los sectores dentro del disco, el tamaño de los sectores y un listado de cada uno de los sectores que pueden ser accedidos *(Véase fig. 5.15).*

Figura 5.15. Detalles de la imagen proporcionados por la herramienta Sleuth Kit Autopsy.

En esta herramienta es muy sencillo localizar los archivos que fueron eliminados ya que cuenta con una opción que permite ver todos los archivos que se encuentren en espacios no asignados y que estan dentro de los directorios de la imagen forense *(Véase fig. 5.15)*.

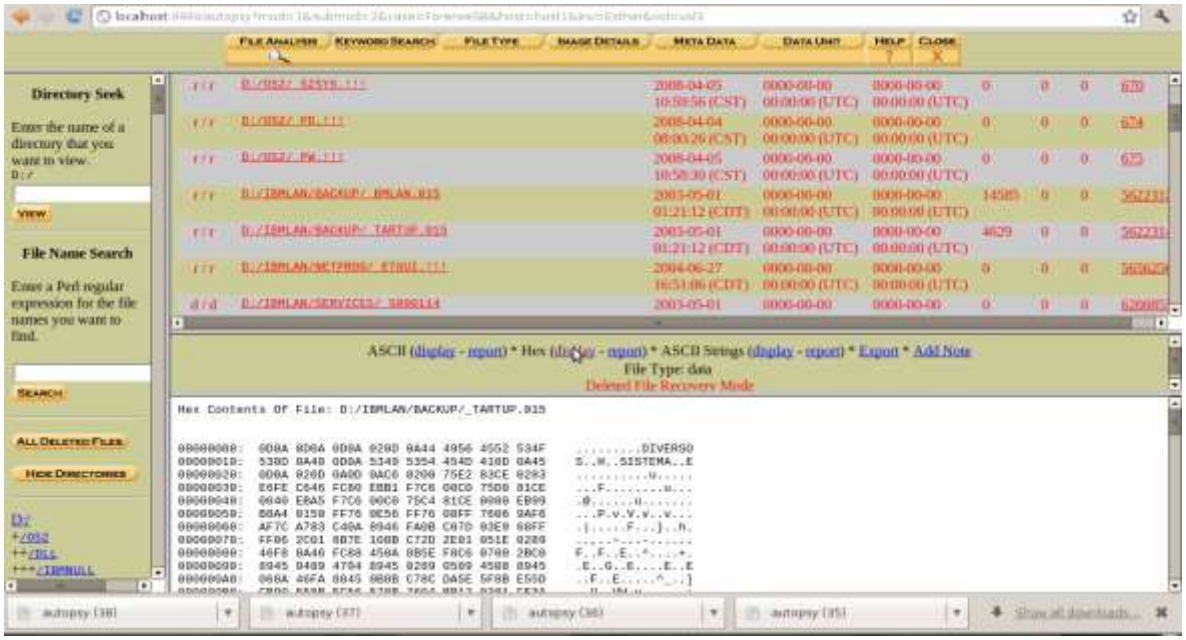


Figura 5.16. Archivos eliminados dentro de la imagen forense.

6.2.3.2 Detección de archivos cifrados.

Lo primero que se analizó es, si la imagen forense contenía algún archivo que hiciera uso de métodos de cifrado *(Véase fig.5.17)*

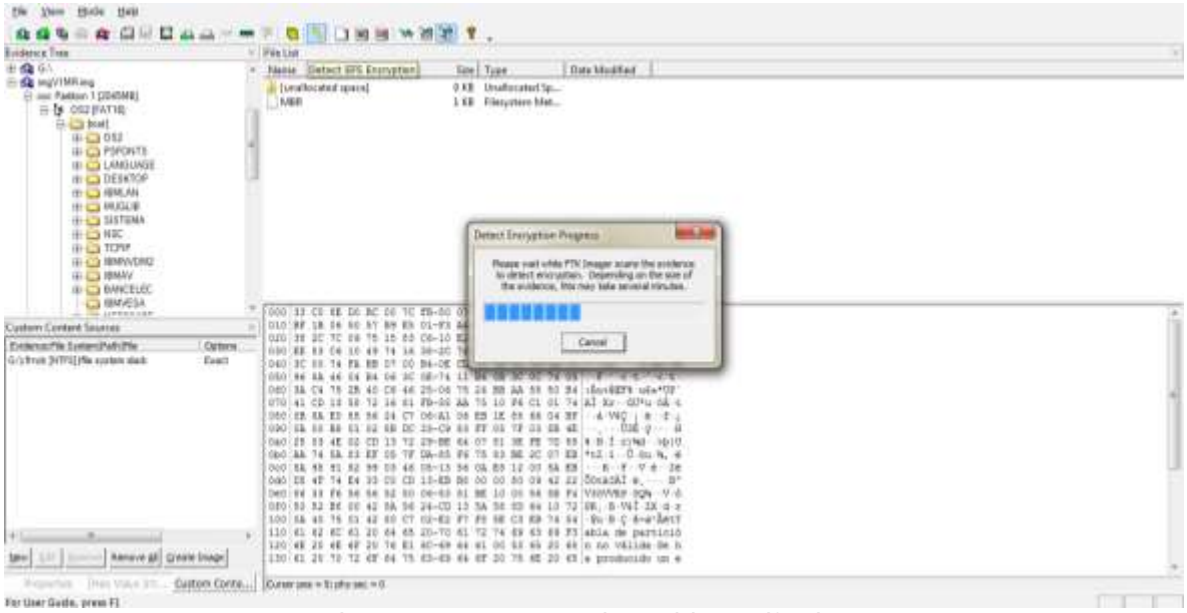


Figura 5.17 Detectando archivos cifrados.

Para poder realizar este análisis se ejecuta dentro de la herramienta la opción de “Detected EFS Encrypted files” –detección de archivos cifrados-, la cual escanea la evidencia notificando al analista si encontró algún archivo cifrado. De haber encontrado algún archivo cifrado lo marcará anteponiendo al nombre del archivo, que aparece en el árbol de evidencia, el icono de una llave.

En este caso al terminar el escaneo de la evidencia no se detectó ningún archivo que hiciera uso de algún método de cifrado.

6.2.3.3 Búsqueda de bitácoras.

Posteriormente se hizo la búsqueda de las bitácoras creadas por el sistema AS sistema encargado de registrar las transacciones hechas en las diferentes sucursales de la institución bancaria.

Las bitácoras creadas por el sistema As ese día se encontraron en un espacio no asignado es decir estas bitácoras habían sido borradas.

Una vez que se encontraron las bitácoras se hizo la extracción de los archivos para poder abrirlos desde un editor de texto.

Dentro de estas bitácoras se encontraron todos los movimientos realizados el día 2 de abril del 2008, el objetivo de estas bitácoras es registrar la actividad de cada terminal.

Para cumplir con ese objetivo cada movimiento se registra con la siguiente información: el día, la hora en que se efectuó el movimiento, la terminal desde la que fue realizado, la clave que identifica al cajero responsable de dicho movimiento y su nombre *(Véase tabla 5.23*).

Tabla 5.23 Distribución de la información dentro de la bitácora que registra los movimientos de cada terminal.

Fecha, hora, clave que identifica al cajero	Nombre del cajero que posee la clave anterior	Terminal desde la que se realiza el movimiento

También se encontró otra bitácora en la cual se registra cada conexión que tienen las diferentes terminales al sistema, esta bitácora se encuentra guardada en el servidor central.

La información que contiene esta bitácora es: una clave alfanumérica única, el tipo de mensaje que manda ya sea informativo o de error, la clave que identifica a la terminal conectada, fecha y hora de la conexión y la descripción de la actividad *(Véase tabla 5.24)*

Tabla 5.24 Distribución de la información dentro de la bitácora que registra las conexiones de las diferentes terminales.

Clave de la actividad	Tipo de mensaje	Fecha y hora	Terminal	Descripción de la actividad

Al analizar estas dos bitácoras se encuentra que los tiempos coinciden, es decir coincide que en el momento en el que se encuentran registrados los movimientos, la terminal se encontraba conectada al servidor.

En la primera bitácora –bitácora en la que se encuentran registrados los movimientos realizados por la terminal- se puede ver la información correspondiente a los movimientos irregulares.

En esta bitácora se puede ver que los movimientos fueron realizados en un tiempo de, una hora ocho minutos y cincuenta y seis segundos. Registrándose el

primero a las nueve horas con treinta y nueve minutos y cuarenta y un segundos -9:39:41- y el último a las diez con cuarenta y ocho minutos y treinta y siete segundos -10:48:37-.

Mientras que en la segunda bitácora se puede notar que la terminal hizo conexión con el servidor a las nueve horas con treinta y seis minutos y seis centésimas de segundo -9:36:06-, terminando la conexión a las diez horas con cincuenta y tres minutos y tres centésimas de segundo -10:53:03-.

También se puede confirmar que los movimientos fueron realizados bajo la clave de la cajera1 y del subgerente, personas que se encuentran presuntamente inculpadas de estos movimientos.

Para tener los datos de una manera clara y rápida estos son colocados en una línea de tiempo *(Véase fig. 5.18)*.

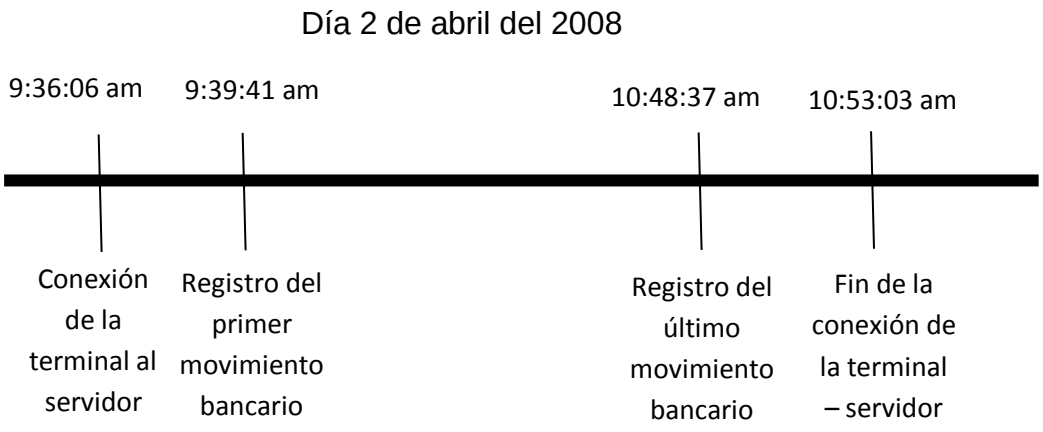


Figura 5.18 Línea del tiempo con el registro de las conexiones al servidor y registro del primer y último movimiento bancario.

6.2.3.4 Análisis de los tiempos para realizar los movimientos bancarios.

Para seguir analizando la información que se encuentra en la bitácora que registra las transacciones hechas por las terminales se pasó la información a un documento Excel, en donde es más fácil poder manejar la información y reorganizarla.

De esta manera se obtuvo un documento que contenía todos los datos de los cuarenta y cinco movimientos irregulares. Con estos datos se pudo calcular la diferencia de tiempo entre cada una de las transacciones efectuadas.

Obteniendo que el tiempo menor entre una y otra transacción fue de cuarenta y seis segundos -46''-, la primera transacción fue realizada a las 10:33:43 y la segunda a las 10:34:29. Es importante mencionar que ambas transacciones requirieron de una doble autorización ya que sobrepasaban el monto que puede autorizar el cajero.

Así también se obtuvo que el tiempo mayor entre una transacción y otra fue de doce minutos con tres segundos -12' 3''- , La primera de ellas se realizó a las 10:08:44 y la segunda 10:20:47. Estas dos transacciones también requirieron de una doble autorización ya que sobrepasaban el monto que puede autorizar el cajero.

Al calcular el tiempo promedio entre una transacción y otra se tienen que en promedio el tiempo que pasa entre una transacción y otra es de un minuto cincuenta y tres minutos -1' 53''-.

Al realizar este análisis se deduce que durante el lapso de tiempo en el que se realizaron los cuarenta y cinco movimientos el cajero no pudo haber estado atendiendo a clientes del banco ya que el tiempo promedio para realizar los movimientos fue de un minuto cincuenta y tres segundos. Por lo que de las 9:39:41 a las 10:34:29 no se pudo haber dado atención a clientes en la ventanilla donde se desempeñaba la cajera1.

6.2.3.5 Análisis de las imágenes del sistema de circuito cerrado de televisión CCTV.

Otro material que se sometió a análisis fueron las imágenes capturadas por el sistema de circuito cerrada de televisión –CCTV-. Estas cintas fueron solicitadas a la institución bancaria, sin embargo no fueron facilitadas argumentando que el sistema se había dañado y no se tenían las grabaciones del día 2 de abril del 2008.

A cambio de estas cintas sólo se entregaron dos imágenes en las que se muestra dos momentos capturados por una cámara que se encontraba a espaldas de los cajeros.

Estas imágenes muestran la caja uno y dos de la sucursal desde la que presuntamente se realizaron los movimientos irregulares. La persona presuntamente culpable se encontraba laborando en la ventanilla 1.

En estas imágenes no se puede ver claramente la cara de la persona que se encuentra en la ventanilla 1, ni se puede afirmar que se trate de una mujer o de un hombre.

Estas dos imágenes según lo dicho por la institución bancaria fue lo único que se pudo rescatar de las cintas del día 2 de abril del 2008. Dichas imágenes fueron entregadas dentro de un archivo PowerPoint.

Al no entregarse las imágenes en su formato original no se pueden considerar como evidencia ya que queda en duda la conservación de su integridad.

Sin embargo estas imágenes proporcionadas fueron sujetas a análisis. Se analizó la información de los metadatos del archivo que contenía las imágenes.

La extracción de metadatos se realizó con la herramienta FOCA una herramienta que entre otras cosas brinda la oportunidad de extraer los metadatos

de archivos. Esta herramienta cuenta con una versión libre que es la que se utilizó para este análisis *(Véase fig. 5.19)*.

Figura 5.19 Extracción de metadatos con la herramienta FOCA.

En la figura 5.19 Se puede ver que al extraer los metadatos del archivo podemos visualizar la fecha y hora de creación y modificación del documento, bajo que usuario fue creado, con que software fue creado, el sistema operativo que se uso en la computadora donde fue creado el documento, el tiempo que le tomó al usuario hacer las modificaciones en el archivo y el título del archivo.

Concerniente a esta investigación los datos que más nos interesa conocer son: las fechas de creación y modificación, el usuario y el tiempo de edición.

En este caso encontramos que el archivo fue creado el 18 de febrero de 2010 a las 2:25:19pm y fue modificado el día 2 de abril de 2010 a las 3:25:41pm, tomándose un tiempo de cinco minutos cincuenta y cuatro segundos -5’ 54’’-para realizar las modificaciones.

Con toda esta información se desecha esta evidencia como una evidencia verídica pues se ha roto su cadena de custodia. Primero al no conservar el formato original del archivo, posteriormente por haber hecho modificaciones al archivo en donde se encuentran las imágenes rescatadas.

Al no conservar la evidencia su integridad esta no servirá para refutar y afirmar nada, por la falta de veracidad que posee.

Una vez descartadas las imágenes como pruebas validas se procedió a analizar otro punto importante dentro del sistema bancario. Este es la información sobre la red.

6.2.3.6 Información de red.

Se realizó el análisis de información de red, aplicaciones instaladas que permitirán acceso remoto al equipo ya que según las declaraciones de la presunta culpable, ella trabajaba cuando de repente se empezaron a generar bauchers que ella no había registrado y mucho menos había recibido dinero de ellos.

Si es que el sistema presentó este tipo de comportamientos, se podría pensar que hubo acceso remoto a la máquina por medio del cual se realizaron los movimientos.

Para poder comprobar o refutar esta teoría se procedió a investigar dentro del sistema archivos que pudieran dar indicio de que el sistema contara con alguna aplicación por la cual se pudiera tener acceso remoto a la máquina.

Mientras se analizaban los archivos contenedores de información sobre la red, se encontró una bitácora que registra la ejecución del comando FORCEDELETE, el cual elimina ejecutables como: ipformat.exe, iptrace.exe, arp.exe, entre otros *(Véase fig. 5.20).*

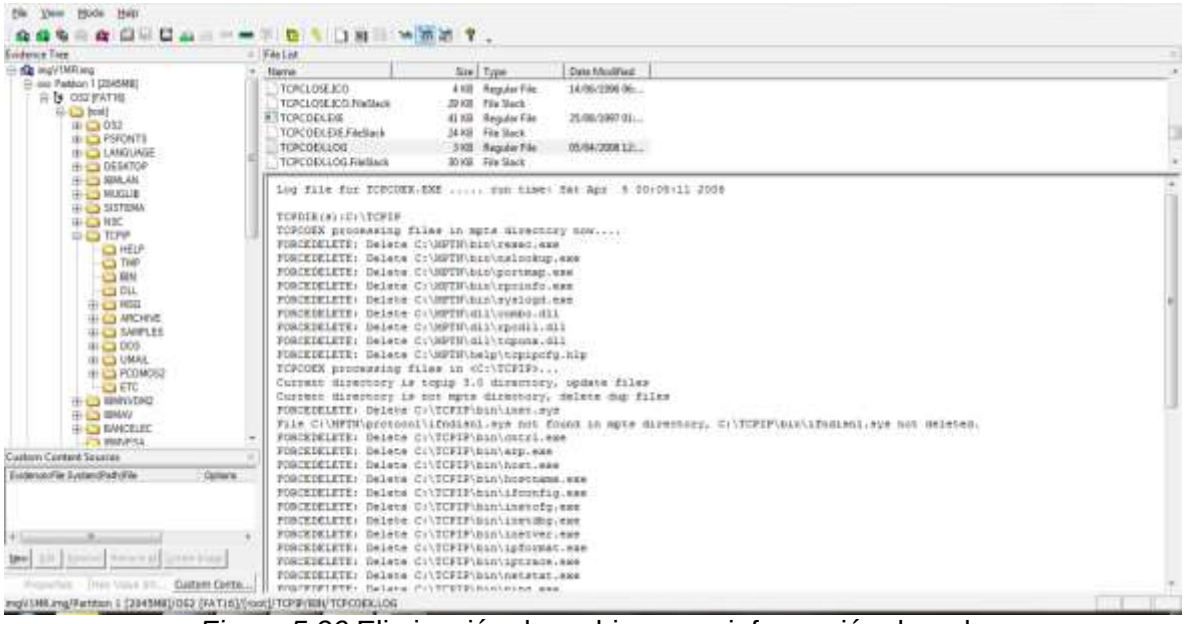


Figura 5.20 Eliminación de archivos con información de red.

También se encontraron bitácoras de una aplicación llamada NetView Dm/2, el cual permite la comunicación de un servidor a otro, así como la administración de software o aplicaciones de manera remota.

La bitácora encontrada en la imagen forense del servidor, muestra que el día 2 de abril del 2008 hubo un registro de conexión *(Véase fig. 5.21)*.

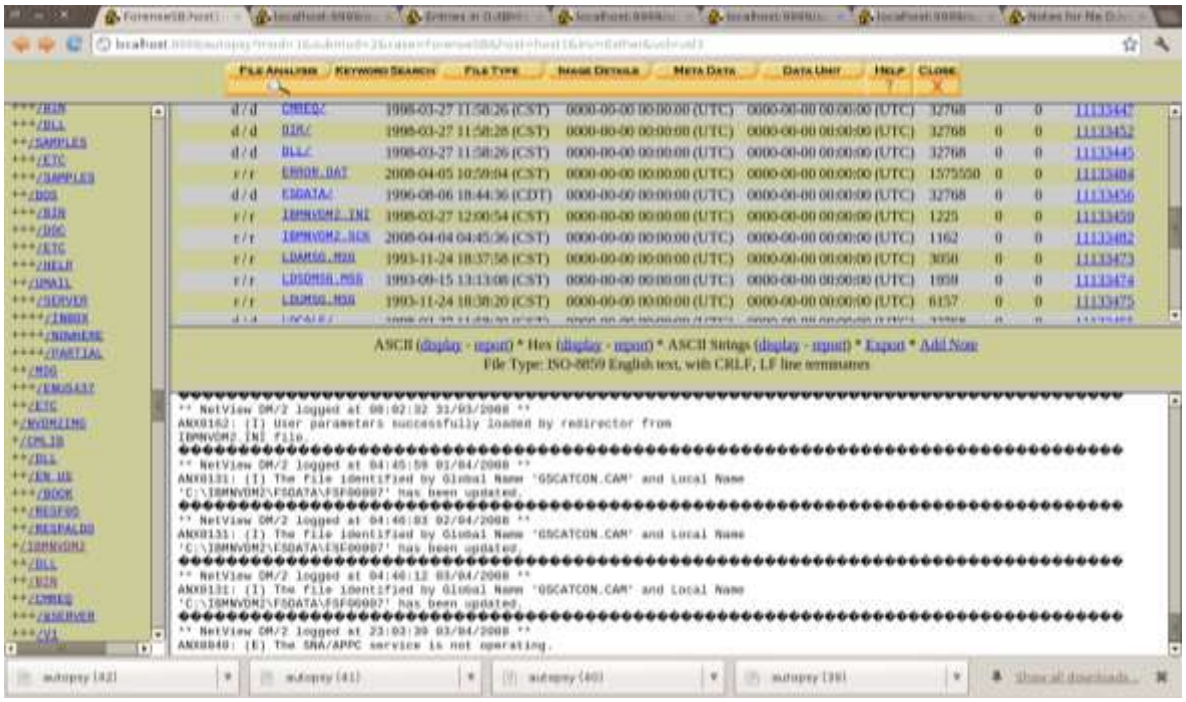


Figura 5.21. Bitácora de la aplicación NetView.

6.2.3.7 Fortaleza de contraseñas.

Por último se analizó el sistema para comprobar la fortaleza de sus contraseñas al momento del incidente.

Según información proporcionada por la institución bancaria, el método de autenticación al sistema es por medio de una contraseña asociada a un nombre de usuario, la cual está limitada a una longitud máxima de cuatro caracteres. Tanto los usuarios como las contraseñas son elegidos por el usuario.

La longitud de cuatro caracteres es muy corta para poder garantizar que una contraseña es segura, la longitud mínima que se recomienda es de ocho caracteres. El doble de longitud que se tiene para admitido en el sistema AS.

Entre menor es la longitud de una contraseña más fácil es lograr la ruptura de ésta. Con una computadora sencilla se puede lograr adivinar la contraseña de una longitud de cuatro caracteres en tan sólo dos minutos y medio, considerando que la contraseña este bien construida.

Para la construcción de las contraseñas el sistema acepta números y letras, por lo que una contraseña puede estar formada por letras mayúsculas, letras minúsculas y números. Sin embargo el sistema no valida que al construir una contraseña el usuario use todas estas variaciones, por lo que se puede tener contraseñas constituidas por puras letras minúsculas o por puros números. Este tipo de contraseñas es sumamente débil.

De igual manera el sistema permite el uso de contraseñas con significado semántico con respecto al idioma español, esto provoca que haya la posibilidad de tener contraseñas susceptibles a ataques de diccionario.

El único punto que valida el sistema es que la contraseña no sea la misma palabra que la del usuario y que no sea la misma que fue asignada.

Dentro de la información proporcionada por la institución bancaria se encontró que el algoritmo utilizado para almacenar las contraseñas cifradas era el algoritmo DES, el cual desde 1999 no es recomendable usar para la protección de datos sensibles pues debido al desarrollo tecnológico es posible hallar la clave en cuestión de horas dependiendo del poder de cómputo que se tenga.

A continuación se presentara la tabla que resume las actividades realizadas en la fase de análisis *(Véase Tabla 5.25, 5.26 y 5.27).*

Tabla 5.25 Resumen de la fase de análisis en la parte de preparación.

Fase de Análisis		
Preparación		
Preguntas claves	¿Es un dato clave?	
Etapas	• Equipo de hardware y software	• Se consideraron dos equipos de cómputo para realizar el análisis de las imágenes forenses. • Los equipos tenían diferentes sistemas operativos para tener la facilidad de utilizar las diferentes herramientas que existe. • Se configuraron los equipos para que estos no dañaran la integridad de la evidencia. • Dentro del laboratorio forense se destinó un lugar seguro para el almacenamiento de la evidencia. • Se siguieron procedimientos para conservar y verificar la integridad de la evidencia durante todo el proceso de análisis.
	• Información previa	• Se contaba con la lista de palabras claves recabadas durante las fases anteriores. • Se contaba con la información proporcionada por la institución bancaria. • Se pudo observar el funcionamiento del sistema. • Se contaba con la declaración de la cajera1 presunta culpable del fraude bancario

Tabla 5.26 Resumen de la fase de análisis en la parte de análisis.

Fase de Análisis		
Análisis		
Preguntas claves		¿Es un dato clave?
Etapas	• Búsqueda de datos	• Se emplearon diferentes herramientas para ver el contenido de las imágenes forenses. • Se examinaron todos los archivos que contenía cada una de las imágenes forense descubriendo los archivos ocultos y borrados. • Se hizo el análisis de los archivos en busca de archivos cifrados. • Se buscaron las bitácoras creadas por el sistema desde el cual se realizaron los movimientos irregulares. • Se realizó el análisis de las imágenes generadas por el sistema de circuito cerrado de televisión. • Se buscaron aplicaciones que permitieran la conexión por red dando la posibilidad de tener acceso remoto al sistema • Se analizó la fortaleza de las contraseñas usadas para autenticarse ante el sistema. • Se usaron las palabras claves que se habían recolectado para encontrar información de una manera más fácil. • Se hizo uso de líneas de tiempo para registrar hechos que acontecieron el día del incidente.

Tabla 5.27 Resumen de la fase de análisis en la parte de recuperación.

	Fase de Análisis	
	Recuperación	
Preguntas claves		¿Es un dato clave?
Etapas	• Extracción de datos	• Se hizo la extracción de las bitácoras producidas por el sistema AS. Estas bitácoras se analizarían más profundamente posteriormente. • Se hizo la extracción de bitácoras relacionadas con aplicaciones instaladas en el sistema que permitían el acceso remoto al mismo. • Se realizó la extracción de archivos borrados que coincidían con la fecha del incidente.

Una vez realizado el análisis de la evidencia se tiene que reportar los resultados a la entidad o persona que haya solicitado los servicios del analista forense.

7. Fase de Creación del reporte

La creación del reporte será la forma de entregar los resultados de la investigación forense. El formato en el que se entreguen estos resultados podrá variar dependiendo de los requerimientos de la entidad que haya solicitado los servicios del analista forense.

En este caso este análisis se realizó porque la parte acusada -cajera1- junto con su abogado creyeron pertinente la realización de esta investigación. Por lo tanto los resultados fueron reportados al abogado.

7.1 Reporte de peritaje.

El abogado solicito al analista forense responder a una serie de cuestionamientos que le ayudarían a armar su defensa. Este cuestionario se creó como resultado de un trabajo conjunto del perito en informática y el abogado.

A continuación se muestran las preguntas a las que se tenía que dar respuesta después de haber realizado la investigación forense. El cuestionario consta de diecinueve preguntas.

1) Dictaminar si el Sistema de Software denominado “AS” de la institución bancaria tiene las fortalezas de seguridad suficientes para prevenir y evitar transferencias de fondos por parte de personas no autorizadas.

2) Dictaminar si el Sistema de Software denominado “AS” de la institución bancaria tiene los huecos o vulnerabilidades de seguridad suficientes para permitir el robo y uso inadvertido de claves para realizar transferencias electrónicas por parte de personas no autorizadas.

3) Dictaminar si los controles de seguridad del Sistema de Software antes mencionado y de las propias instalaciones de la institución bancaria, lugar físico desde el cual se operó el mencionado sistema de software, cumplen con las recomendaciones de seguridad que exigen los estándares internacionales tales como el ISO 17799 y el ISO 27001.

4) Dictaminar si personas con conocimientos en cómputo, software, redes y sistemas computacionales pueden o no vulnerar las medidas de seguridad implementadas en el Sistema de Software denominado “AS” y utilizarlo inadvertidamente para fines fraudulentos.

5) Dictaminar si personas no autorizadas pueden acceder a las instalaciones de la institución bancaria –matriz- y de su sucursal, lugar físico desde el cual se operó el mencionado sistema de software.

6) Dictaminar si, con los argumentos y evidencias informáticas expuestas por la institución bancaria y sus peritos, es posible que los C.cajera1 y subgerente hayan podido realizar en lugar, tiempo y forma, las transferencias fraudulentas de las cuales se les acusa.

7) Dictamine si existen fundamentos técnicos y teóricos para relacionar, de manera incontrovertible, una contraseña, clave o password con la persona que la utiliza.

8) Dictaminar si la institución bancaria cumplía, a la fecha de los hechos, con las auditorías que la Comisión Nacional Bancaria y de Valores realiza anualmente a las instituciones de su tipo y con las recomendaciones que dicha comisión emite. En particular si cumplía, a la fecha de los hechos, con las auditorías y sus recomendaciones al sistema AS.

9) Dictaminar si, conociendo las claves necesarias, es indispensable el ingresar al sistema desde los equipos involucrados, o, en su caso si el sistema AS permitía, a la fecha de los hechos, que cualquier persona ingresara con la calidad de cajero o subgerente al mismo desde cualquier equipo de la sucursal en cuestión u otra. En su caso indique si el personal de informática de la Institución bancaria podría ingresar, a la fecha de los eventos desde sus propias terminales utilizando las claves de cajeros, subgerentes o gerentes.

10) Dictaminar si los argumentos y evidencias informáticas, fotográficas y de videograbación expuestas por la institución bancaria y sus peritos coinciden en lugar, tiempo, forma y circunstancia con las ubicaciones, tiempos, formas y circunstancias de los inculpados, en el intervalo de tiempo durante el cual se realizaron las operaciones presuntamente fraudulentas y permiten concluir que los hoy inculpados realizaron efectivamente las operaciones cuestionadas, y, en su caso indique si las declaraciones de los peritos presentados por la institución bancaria están debidamente fundadas en los hechos y las técnicas periciales internacionalmente aceptadas.

11) Dictaminar si existe evidencia para demostrar que las operaciones fraudulentas imputables a los acusados fueron en realidad realizadas por un proceso o programa de software, sembrado en los equipos y programas de la institución bancaria por terceras personas, y no por los inculpados.

12) Dictaminar si se ha modificado en algún momento el medio de identificación electrónica otorgado a los inculpados, en caso afirmativo indicar en qué fecha, desde que equipos fue realizado esa modificación, quienes pueden realizarla y que claves se requieren para ello.

13) Dictaminar si pudo un tercero por medios presenciales o remotos operar los equipos involucrados en el fraude habiendo capturado las claves necesarias.

14) Dictaminar si se pueden realizar operaciones remotas desde los equipos involucrados, y en su caso, expresar que mecanismos pueden utilizarse para ello y si existe instalado en los equipos involucrados o cualquier otro de la sucursal el software necesario a esos efectos.

15) Dictaminar si hubo la posibilidad de operar los equipos en forma remota, bajo las condiciones de seguridad informática vigentes a la fecha del suceso.

16) Dictaminar, por medio del análisis forense de los registros de la Institución Bancaria las bitácoras de operación completas de las reparaciones realizadas al cajero automático de la sucursal para demostrar las actividades de los sujetos a proceso.

17) Dictaminar y explicar cuál es el procedimiento necesario para llevar a cabo las reparaciones del cajero automático y si se requiere la presencia de alguna persona a esos efectos, en su caso, cuáles serían esas personas y si existen claves o identificadores para esa operación.

18) Dictaminar, de acuerdo al punto anterior sobre la presencia de alguno o ambos inculpados en el cajero automático al momento en que ocurren las operaciones bajo análisis.

19) Explicar cuáles son las funciones del programa Team Viewer y otros similares y dictaminar si alguno de ellos se encuentra instalado en los equipos involucrados o cualesquiera otro de la sucursal, y, en su caso obtener los archivos de registro de su utilización explicitando las fechas y las horas en que fue activado.

Ya que se contaban con el cuestionario que ayudaría al abogado a armar su defensa. Se procedió a dar respuesta a cada uno de los puntos con la información obtenida durante la fase de análisis.

Al contestar cada uno de los puntos estos deben de estar fuertemente sustentados en evidencia encontrada durante el análisis.

Es importante mencionar que para responder a los puntos planteados anteriormente el perito en informática o analista forense debe de permanecer en una posición imparcial y mostrar los resultados que su investigación arrojo.

Estos resultados se encuentran en el Anexo 1 “Reporte de peritaje”. Estas respuestas conformaron parte del reporte entregado.

7.2 Reporte Técnico.

En el reporte técnico se mostrara el análisis de las medidas de seguridad y vulnerabilidades del sistema AS de la institución bancaria. Este reporte tiene como objetivo fundamentar algunas de las respuestas dadas en el anterior reporte -Reporte de Peritaje-

Anexo Técnico.

El presente Anexo Técnico analiza las principales vulnerabilidades de seguridad y sus consecuencias en escenarios de ataques del Sistema de Software denominado “AS” Este análisis se fundamental en el estudio especializado en seguridad que el Perito realizó directamente en la diligencia de recreación del Sistema de Software mencionado realizada el día 13 de Agosto de 2009 en las oficinas de la institución en los manuales de operación y en la descripción que sobre el mismo le fueron proporcionado por los representantes de la Institución Bancaria.

Sección 1.1.- Vulnerabilidad del Sistema de Software denominado “AS” versión “38.5”, por carecer del Concepto de Firma Digital.

Las medidas de seguridad con las que cuenta el sistema de la Institución Bancaria mediante el software “AS” son susceptibles de ser vulneradas. Una de las razones de lo anterior se debe a que el proceso de realización y autorización de una operación se lleva a cabo con base en usuario y contraseña o clave asociada a ese usuario. La utilización de una contraseña o clave como base de seguridad para demostrar que una persona sea quien dice o debe ser y que, en base a eso, haya realizado, con esa clave o contraseña, una acción específica, no tiene fundamento alguno ni técnico, ni científico, ni teórico, ni práctico.

Las citadas contraseñas que usa el sistema pueden ser adquiridas o robadas por una persona no autorizada o proceso de cómputo para acceder y operar de manera ilícita el sistema y realizar con ellas acciones maliciosas tales como fraudes.

En seguridad informática, un proceso de ***firma digital*** (ya sea de un mensaje o, en este caso, de una transacción) se realiza mediante una transformación matemática que depende del contenido, del mensaje o transacción en este caso, y

de un factor de autenticación (una llave privada criptográficamente fuerte) que autentica al usuario como legítimo y que lo relaciona con la operación. Esta transformación es única y sólo puede ser realizada por la persona que relaciona la operación con la llave privada. De esta forma la identidad de la persona queda relacionada con el proceso.

Además, en el concepto de ***firma digital***, para validar la legitimidad de la operación, el verificador de tal operación debe poseer y usar para tal verificación, un certificado de llave pública expedido y firmado digitalmente por una Autoridad Certificadora confiable. La llave pública, que la aplicación extrae del Certificado Digital, una vez corroborada la validez del firmante que lo expide, está relacionada matemáticamente con la llave privada que el usuario legítimo usó para realizar la transacción. Si esta verificación de la ***firma*** es válida se acepta la transacción como legítima, es decir, como realizada realmente por el poseedor único de la llave privada, de lo contrario se rechaza.

Este concepto de ***Firma Digital*** no está implementado en el sistema de la Institución Bancaria mediante el software “AS” lo cual lo hace susceptible a todos los riesgos de suplantación de usuarios legítimos.

Para mejor comprender el concepto de firma y el problema que nos ocupa, a continuación se hará una analogía con la firma autógrafa (la que se realiza sobre papel).

La firma autógrafa contiene algo inherente a la naturaleza del firmante, es independiente del documento (siempre se realiza la misma firma en cada documento, o casi idéntica, sin contar los factores humanos que la alteran), es intransferible, es no reusable, entre otras supuestas características.

En la firma digital, las características anteriores no son supuestas, son reales. También es intransferible (sólo puede ser realizada por el firmante), contiene algo inherente al firmante. Pero, a diferencia de la firma autógrafa, es dependiente del documento. Es decir, si el documento sufriera cualquier tipo de alteración o modificación el resultado de la firma será totalmente diferente.

Por lo tanto, una contraseña o clave, como el que utiliza el sistema de software “AS” no es un mecanismo seguro ya que, si ésta contraseña es robada o copiada, puede utilizarse como si se tratara de un usuario auténtico, debido a que una contraseña no contiene nada inherente al usuario. Esto le permite a cualquier “usuario malintencionado” iniciar, realizar y concluir con éxito un proceso fraudulento de traspaso de fondos.

Debido a que el sistema no cuenta con un proceso de firma digital, sino con una forma de acceso y autorización mediante usuario y contraseña, presenta una grave debilidad, mediante la cual, personas ajenas a los usuarios legítimos o autorizados de dicho sistema pueden tener acceso al sistema de “AS””, mediante la adquisición o captura de las contraseñas y de los usuarios autorizados.

A continuación se describirán lagunas de las técnicas y procedimientos más comunes para la captura ilícita, robo u obtención de nombres de usuario y sus correspondientes claves o contraseñas

Sección 1.2.- Técnicas y Procedimientos de Captura de Información sensible (nombre usuario y contraseña) en el Sistema de Software denominado “AS”

Existen varios y diversos modos, técnicas y procedimientos para obtener ilícitamente, por parte de personas no autorizadas, la información sensible (*nombre usuario* y *contraseña* o clave) del sistema “AS”, el cual no cuenta con los candados o mecanismos de seguridad para evitarlo. Algunas de estas técnicas y procedimientos son las siguientes:

1) Inyección o Instalación de Código Malicioso para obtener información sensible del sistema durante su operación.

2) Utilización de programas de ruptura de contraseñas llamados “crakers” para adivinar contraseñas débiles, tales como las utilizadas por el sistema “AS”.

3) Instalación de programas escucha llamados “sniffers” para obtener información sensible (*nombre usuario* y *contraseña* o clave) del sistema “AS”.

4) Técnicas de Ingeniería Social para obtener información sensible (nombre usuario y contraseña) de los usuarios legítimos

Subsección 1.2.1: Inyección o Instalación de Código Malicioso para obtener información sensible del sistema durante su operación

Es posible sustraer información (almacenada, en tránsito, o que se esté generando), sin consentimiento del usuario autorizado mediante la inyección remota o instalación directa de lo que genéricamente se denomina Código Malicioso o “Malware”. Un tipo común y de uso generalizado de Código Malicioso o “Malware”, para lograr el objetivo de sustraer o capturar información sensible (nombre usuario y contraseña) del sistema, son los programas de software y hardware llamados “keyloggers”.

Un keylogger es un programa de tipo hardware o de tipo software que captura, registra y almacena todos los caracteres del teclado de un equipo de cómputo pulsados por el usuario u operador de tal equipo de cómputo. Igualmente captura, registra y almacena todos los eventos o “cliks” del “mouse” o ratón que pulse el usuario u operador de tal equipo.

Estos programas de software o hardware son instalados, en menos de un minuto, directamente por un empleado o persona con aceso al área física donde se encuentra el equipo de cómputo que se desea intervenir, por cualquier empleado con acceso al sistema o al equipo, o por un intruso que ingresa inadvertidamente al área física donde se encuentra tal equipo de cómputo, aprovechando la falta de controles de seguridad en el acceso a tales áreas.

Igualmente estos programas se pueden autoinstalar en el equipo de cómputo cuando este equipo se conecta a la red, ya sea directamente o usando como medio de transporte cualquier archivo que se baje de la red, o bien un virus informático. En el caso del sistema “AS” esto es posible porque se trata de un sistema que opera en red y consta de un proceso cliente y de un proceso servidor, cada uno de ellos ejecutándose en equipos de cómputo distintos pero dentro de la misma área física.

Una vez instalado en el equipo de cómputo, un “keylogger” se ejecuta en modo invisible. Es decir, el usuario u operador del equipo de cómputo puede estar trabajando frente a la computadora sin percibir que hay tal programa nuevo y desconocido por él. Estos programas maliciosos tienen características que facilitan su uso.

Un “keylogger” crea y mantiene un archivo de almacenamiento de actividad o de bitácora (en donde cada carácter pulsado y cada evento o “click” del “mouse” o ratón, o cada aplicación que sea abierta o utilizada por el usuario u operador del equipo, quedará almacenada en un registro bajo el control del “keylogger” y, en última instancia, bajo el control de la persona que lo instaló o pidió que lo instalara). Lo anterior sucede para cada usuario registrado en el Sistema Operativo o Aplicación que se esté ejecutando (para el caso del presente análisis, el Sistema Operativo es core OS/2 de la compañía IBM y de la aplicación denominada “AS”), lo que permite hacer una separación de resultados de acuerdo a los usuarios. Un “keylogger” también hace capturas de pantallas del equipo de cómputo en que está instalado una vez cada segundo o cada vez que una nueva aplicación o pantalla es desplegada. A través de estas pantallas se puede observar también la información capturada.

Otra característica de estos programas maliciosos es que permiten analizar sus registros en bitácora de acuerdo a un calendario, donde se pueden seleccionar los datos obtenidos por día, por días de la semana, los datos del último mes, los más recientes, sólo los registros sin leer, etc. Esto permite la facilidad de instalar el “keylogger”, dejarlo funcionar durante días, semanas o

meses y revisar sus bitácoras sólo hasta que se considere conveniente. Es decir, hasta que ya se haya capturado la información de interés o hasta cuando no se corra ningún peligro de ser descubierto.

Estos programas maliciosos se pueden conseguir de manera gratuita en la red Internet en sitios tales como los siguientes:

www.relytec.com

www.spytech-web.com

www.refog.com

www.amplusnet.com

www.widestep.com

www.eltima.com

www.cromosoft.com

http://www.keylogger123.com

Sólo se debe bajarlos de la red e instalarlos en el equipo de cómputo de interés.

También se pueden adquirir en hardware del tamaño de una memoria flash USB por un costo que va desde los 30 (treinta) dólares USA.

Las siguientes son algunas direcciones de empresas donde se pueden adquirir estos dispositivos:

http://www.milestonesafety.com/keykatcher.html

http://keyspyer.com/products/KeySpyer_PS2_Standard_64k

http://www.keyghost.com/

http://www.keydevil.com/

http://www.keelog.com/

http://www.exploreanywhere.com/hrd-features.php

http://www.keyghost.com/ *(compatible para sistemas OS/2)*

Para el caso de su presentación en hardware, el dispositivo se conecta entre el cable del teclado y el puerto PS/2 o el puerto USB (según se conecte el teclado), permitiendo su uso sin que los usuarios de esos equipos de cómputo se percaten de ello. Este hardware realiza capturas, de todo carácter que se pulse en el teclado del equipo de cómputo o de cada evento o click del mouse, desde que el equipo de cómputo se enciende hasta que sea apagado. En caso de que el "keylogger" se deje instalado durante varios días, generará nuevos registros (es decir, no se sustituirán los datos que han sido capturados, sino que almacenará los nuevos registros como si se tratara de un nuevo archivo).

A continuación se mostrará un ejemplo del funcionamiento de uno de estos programas "keylogger", con el fin de comprender mejor su uso y operación.

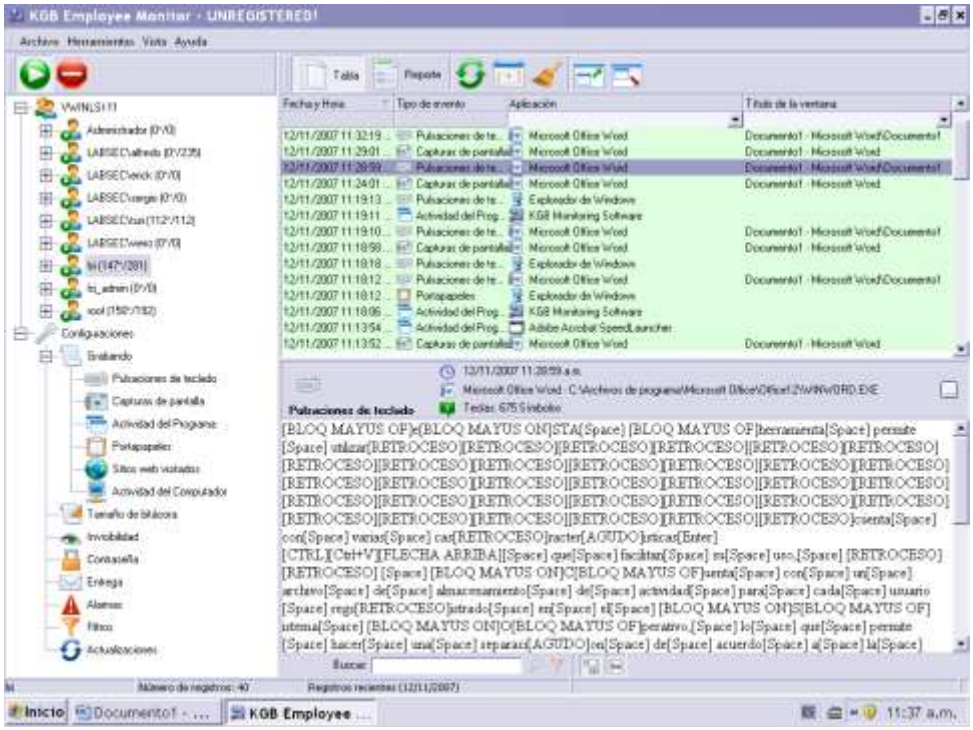


Figura 5.27 Pantalla de captura de información mostrando uso de programa "keylogger".

En la Fig. 5.27 se observa en pantalla la manera en que el usuario denominado ***lsi*** (sombreado en la columna del lado izquierdo), usando la aplicación Word de Microsoft Office (sombreada en la fila superior derecha), escribió el siguiente texto (mostrado en los renglones inferiores de la derecha): "…*con varias características que facilitan su uso. Cuenta con un archivo de almacenamiento de actividad para cada usuario registrado en el Sistema Operativo, lo que permite hacer una separación de acuerdo a la*…".

Lo que se demuestra mediante la visualización de la pantalla mostrada en la Fig. 5.27 es cómo cada uno de los caracteres digitados en el teclado queda registrado por medio del programa malicioso "keylogger" para su posterior análisis.

A continuación se mostrará el uso de este programa "keylogger" capturando un *nombre de usuario* y su correspondiente *contraseña* o clave.

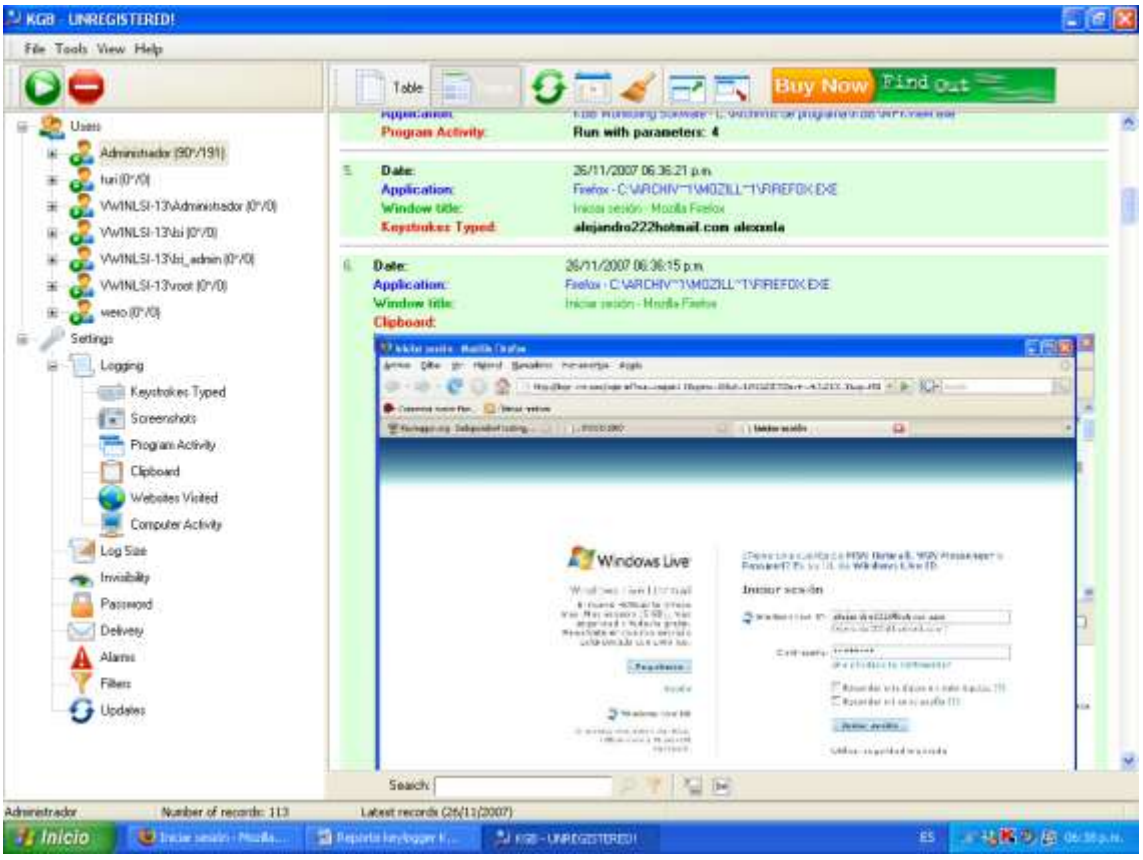


Figura 5.28. Pantalla captura usuario y contraseña usando herramienta keylogger.

En la Fig. 5.28, se observa la pantalla capturada por el programa “keylogger” mediante la cual el usuario *Administrador* (sombreado en la columna izquierda). La actividad de este usuario es registrado por el “keylogger” mientras se encuentra navegando en Internet. Esto sucedió al teclear el nombre de su usuario y su correspondiente contraseña, en la página de *Hotmail.com* (para poder accesar a su correo).

Esta información quedó almacenada en el registro del programa “keylogger” (columna derecha), la cual se observa en el campo número 5, frente a la línea *Keystrokes Typed* (Teclas presionadas), con la siguiente información: *alejandro222hotmail.com alexxela*, donde *alejandro222hotmail.com* es el nombre del usuario y *alexxela* es su contraseña.

En la imagen instantánea de ese momento de captura se observa que la información capturada se encuentra marcada con asteriscos (*). Esta información (tanto la instantánea de la pantalla como la captura del usuario y contraseña difieren en centésimas de segundo, como se observa en la imagen).

Subsección 1.2.2: Uso de programas de ruptura de contraseñas llamados “crakers” para adivinar claves o contraseñas débiles, tales como las utilizadas por el sistema de software “AS” de la Institución Bancaria

Otra forma de obtener información sensible, tal como *claves* o *contraseñas* que utilizan los sistemas de software, como el de “AS”, es mediante el uso de programas de software genéricamente conocidos como “crackers”, rompedores o adivinadores de *claves* y *contraseñas* débiles, tales como las que utiliza el sistema antes mencionado para autenticar al usuario ante la institución bancaria y para realizar y autorizar operaciones bancarias tales como depósitos.

Una clave o *contraseña* se dice que es débil cuando en su diseño y construcción intervienen sólo un reducido número de caracteres y el tipo de

caracteres elegidos, de tal forma que las cadenas (*claves* o *contraseñas*) formadas con esos caracteres o números es fácilmente adivinable. Por ejemplo: la cadena *sesamo* formada de 6 caracteres alfabéticos es débil porque la cadena forma una palabra con sentido semántico, la cual existe en el diccionario de la lengua española. Adivinar este clave o *contraseña* le toma a cualquier equipo de cómputo básico actual el fabuloso tiempo de *5 segundos.*

El adivinamiento de esta clave o *contraseña* se hace mediante la implementación de un ataque conocido como *diccionario,* en el cual se prueban como posibles *claves* o *contraseñas* las palabras que existen en un diccionario del idioma español, que son alrededor de 50 mil palabras. Un equipo básico actual prueba *claves* o *contraseñas* a razón promedio de 10 mil por segundo. Entonces el cálculo de los 5 segundos es elemental.

Un ataque de este tipo también puede ser hecho utilizando programas "crackers" que se bajan de forma gratuita de Internet. Un programa "cracker" muy popular es el conocido con el nombre de "*John the Ripper*".

Estos programas prueban todas las posibles *claves* o *contraseñas,* construidos mediante reglas que se le indican explícitamente al programa "cracker", directamente en el sistema que se trate, hasta adivinar el correcto.

Por ejemplo, se le puede indicar al programa "cracker" que pruebe con *claves* o *contraseñas* construidas con fechas de nacimiento de 6 caracteres, donde los primeros dos caracteres representen el año, los siguientes dos caracteres representen el mes y los dos últimos caracteres representen el día. Un posible clave o *contraseña* de este tipo, adivinable en segundos por un equipo de cómputo actual, sería la cadena **580511** correspondiente a una persona que nacida el 11 de Mayo de 1958.

De acuerdo a la información proporcionada por funcionarios y representantes de la institución bancaria al perito, que el perito constató en la diligencia de recreación del sistema realizada el día 13 de Agosto de 2009 en las oficinas de la institución bancaria y la información que obra en los manuales de operación y

características del sistema “AS” las *claves* o *contraseñas* que utiliza este sistema para autenticar o identificar a los usuarios ante la institución bancaria y para realizar y autorizar transferencias de fondos son *claves* débiles, de 4 caracteres alfanuméricos.

Las debilidades concretas del sistema de software “AS” respecto a los “*claves”* o *contraseñas,* son las siguientes*:*

1) El uso de *claves* o *contraseñas* débiles
2) La construcción de los *claves* o *contraseñas* **sí** está limitada en su longitud a un máximo de 4 caracteres, en ambos casos elegidos por el usuario. Esto constituye una gran vulnerabilidad del sistema, ya que el usuario puede definir *claves* o *contraseñas* muy cortas y el sistema se lo permite, creando con ello un gran hueco de seguridad. Entre menor sea la longitud de la clave elegida, menor es el tiempo de ruptura o adivinación del mismo. Por ejemplo, para un clave o *contraseña* de 2 caracteres, una computadora laptop o PC actual sólo requiere de 2 segundos para probarlos todos y adivinar el correcto. Para uno de 3 caracteres, la misma máquina necesita de 26 segundos para adivinar el correcto; para uno de 4 caracteres, necesita 2 minutos y medio. Y todo esto considerando que los *claves* o *contraseñas* estén bien construidos, lo cual no es el caso en la realidad, tal como se explica en el punto 3 siguiente.

El siguiente es un fragmento extraído de la contestación que da el grupo financiero

> *“Las contraseñas son de carácter alfanumérico, de 4 dígitos, se menciona que esta longitud cambiara dependiendo de su identificador de usuario asociado”.*

3) Las *claves* o *contraseñas* se pueden construir de letras mayúsculas, letras minúsculas y números. Pero, en la realidad de la práctica, el sistema no valida esta política de construcción de *claves* o *contraseñas*. En la práctica,

el sistema permite el uso de letras y números en cualquier orden, cadenas todas del tipo atacable por un programa "cracker", susceptibles de ataques de ingeniería social, o por combinación de ambos ataques. Las técnicas de ingeniería social se describirán en la Subsección 1.2.4 de este mismo Nexo Técnico del presente reporte de peritaje.

4) El sistema de software "AS" no valida y no exige, proactiva e interactivamente, que los "*claves"* o *contraseñas* que, aún dentro de las limitaciones de los puntos 2 y 3 anteriores, son definidos por el usuario, estén bien construidos. Es decir, que incluyan en su construcción todos los tipos de caracteres permitidos y que la cadena resultante como clave o *contraseña* no tenga significado semántico respecto al idioma español. Esto se debe exigir para hacer infactibles los ataques mencionados con anterioridad en esta misma sección, principalmente el de diccionario y los realizables con programas "crackers".

5) El punto 4 anterior es de vital importancia para la seguridad de un sistema que basa su seguridad en *claves* o *contraseñas* ya que, de validar la construcción de *claves* o *contraseñas* como se indica en ese punto, la cantidad de posibles *claves* o *contraseñas* que habría que probar en un posible ataque, de los mencionados en ese punto, se haría infactible en el tiempo. Por ejemplo: todos las posibles *claves* o *contraseñas* de 6 caracteres, construidos como se indica, serían alrededor de 4 billones de ellos y un equipo de cómputo básico actual tardaría más de 1 año en adivinar el correcto, ejecutando un programa "cracker". En el caso de "*claves"* o *contraseñas* de 8 caracteres, construidos como se indica, serían decenas de miles de billones de ellos y un tal equipo se tardaría alrededor de 66 mil años en adivinar el correcto.

6) El algoritmo utilizado para transformar la clave o contraseña, una vez que este haya llegado al servidor viajando en claro, es el DES (“Data Encryption Standad”) el cual desde la década de los noventa ya no es recomendable su uso para la protección de datos sensibles, pues debido al desarrollo tecnológico es posible hallar la clave en cuestión de horas dependiendo del poder de cómputo que se tenga. El estándar mundial actual, desde el año 2000 a la fecha, para este tipo de aplicaciones es el algoritmo AES (“Advanced Encryption Standard”). Este algoritmo no se utiliza en el sistema “AS”.

7) La debilidad fundamental, sólo respecto a *claves* o *contraseñas*, del sistema de software “AS”, es que la autenticación e identificación de las persona legítimamente autorizadas para realización y autorización de las transacciones se basa en *claves* o *contraseñas*, descritas anteriormente. Y el uso de *claves* o *contraseñas* de ninguna manera prueban y garantizan que la persona que realiza la transacción sea la que se supone que es, o que debe ser. Como ya se probó con anterioridad en este mismo reporte, las *claves* o *contraseñas* se pueden capturar, adivinar o conseguir sin el consentimiento y conocimiento del supuesto propietario y con ello suplantar a las personas supuestas como legítimas propietarias o responsables de tales *claves* o *contraseñas*.

8) Para que un sistema del tipo de “AS” y la institución bancaria, puedan garantizar y comprobar fehacientemente que una persona determinada fue la que realmente realizó o autorizó una operación, el sistema debe implementar, como base de seguridad, el concepto de *Firma Digital*, ya descrito en la Sección 1.1 de este mismo Anexo Técnico, y mecanismos basados en biometría tales como la huella dactilar, iris del ojo humano o DNA, lo cual es perfectamente viable de implementar en sistemas de software de este y otros tipos.

9) El sistema de software “AS” no implementa verdadera Firma Digital, no implementa mecanismos de seguridad basados en Biometría, como los mencionados en el punto 7 anterior, como base de seguridad para la realización y autorización de las transacciones.

10) Es tal la debilidad de los sistemas de software basados en *claves* o *contraseñas,* que estos ya entraron en desuso y obsolescencia desde hace por lo menos 3 años para sistemas de software con altos requerimientos de seguridad, de los cuales el sistema “AS” es un ejemplo.

Es importante señalar en este punto y momento que los funcionarios y representantes de la Institución Bancaria proporcionaron al perito información sobre la forma en que los *claves* o *contraseñas* son validados en el servidor central de la Institución

Del estudio y análisis de esta información, el perito da las siguientes conclusiones a este respecto.

1) La clave o contraseña, al llegar al servidor después de viajar en claro (sin protección) por la red, se transforma con el algoritmo DES, operando como si fuera una Función Hash. De esta transformación se obtiene un resultado equivalente a una huella digital (por su semejanza con la huella dactilar), el cual se compara con el resultado que se mantiene almacenado en el servidor.
2) Esta forma de “proteger” las claves o contraseñas durante su almacenamiento en el servidor es totalmente débil ya que se pueden adivinar o conocer esas claves o contraseñas diseñando e implementando lo que se conoce como un ataque diccionario sobre toda la base de datos o sobre alguna contraseña en particular.
3) Este ataque lo puede realizar cualquier persona que tenga la base datos de contraseñas cifradas o cualquier persona que tenga acceso al sistema en

su aplicación servidor. En este caso específico, por todos los administradores y personal de operación y mantenimiento del sistema “AS”.

4) Por tanto, el o los administradores del sistema de software “AS” tienen o tuvieron acceso a las claves o contraseñas cifradas. Por lo anterior, y dadas las múltiples debilidades del sistema, pudieron haberlos extraído y haberlos usado de manera ilícita. O bien, pudieron haber vendido o proporcionada toda o parte de la base de datos citada a la delincuencia organizada o a personas específicas para realizar actos fraudulentas con esa información.

Subsección 1.2.3: Uso de programas de escucha, llamados “sniffers”, para obtener información sensible (nombre usuario y contraseña) del sistema en el Sistema de Software “AS” de la Institución Bancaria.

Un programa de escucha llamado **“*sniffer*”,** es un programa fisgoneo y captura de las tramas de red. Generalmente se usa como auxiliar en la administración de la red, aunque también puede ser utilizado con fines maliciosos.

Es algo común que el medio de transmisión (cable coaxial, UTP, fibra óptica, cable telefónico etc.) de una red sea compartido por varias computadoras y dispositivos en la red, lo que hace posible que un equipo de cómputo capture las tramas de información no destinadas a él. Aunque el medio no sea compartido, es posible invadirlo para capturar aquellas tramas destinadas a otro usuario. Para conseguir esto, el programa escucha llamado “*sniffer*” pone la tarjeta de red en un estado conocido como "modo promiscuo" en el cual son capturadas y analizadas las tramas no destinadas al identificador (conocido como MAC address de la tarjeta) del destinatario final de esa trama o paquete. De esta manera se puede obtener todo tipo de información de cualquier aparato o equipo de cómputo conectado a la red, tales como claves o contraseñas y nombres de usuarios enviadas en claro (como es el caso del sistema“AS”), correo electrónico,

conversaciones de chat o cualquier otro tipo de información personal (por lo que son muy usados por atacantes o delincuentes informáticos).

Actualmente existe una gran variedad de estos programas en Internet, algunos se pueden conseguir de manera gratuita en sitios tales como los siguientes:

http://www.snoopanalyzer.com/

http://www.wireshark.org/

http://www.analogx.com/CONTENTS/download/network/pmon.htm

http://www.objectplanet.com/probe/

http://www.snapfiles.com/get/sniphere.html

http://www.netstumbler.com/

http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/PlasticSniffer.shtml

También existen versiones comerciales, algunas direcciones de estos sitios son las siguientes:

http://www.tamos.com/products/commview/

http://www.colasoft.com/

http://www.etherdetect.com/

http://www.microolap.com/products/network/pssdk/order/

La utilización de programas de escucha llamados “sniffers”, permite obtener la información intercambiada entre las entidades que comparten alguna infraestructura de red, sean autorizadas o no.

Un “sniffer” es un monitor pasivo. Es decir, sólo recolecta la información del medio que comparte con otros equipos, esto hace que sea comúnmente imperceptible para los administradores de red.

Las principales vulnerabilidades de seguridad que trae consigo la recolección de información por un “sniffer” son las siguientes:

1) Obtener claves o contraseñas e información sensitiva utilizan protocolos de comunicación y aplicaciones de software, tales como “AS” que transmiten información por el medio sin la utilización de algún mecanismo de seguridad durante el viaje.

2) Hábitos de los usuarios bajo vigilancia, que permiten suplantar a un usuario legítimo al adueñarse ilegítimamente de sus claves o contraseñas.

Subsección 1.2.4: Uso de Técnicas de Ingeniería Social para obtener información sensible (nombre usuario y contraseña) de los usuarios legítimos del Sistema de Software “AS” de la Institución Bancaria.

En seguridad informática se considera a la Ingeniería Social como una amenaza, a menudo subestimada pero regularmente explotada, para tomar ventaja sobre lo que desde hace muchos años se ha considerado el factor más débil de la seguridad de una organización: el factor humano.

La ingeniería social es la práctica de obtener información confidencial mediante la manipulación de usuarios legítimos. Un practicante de la Ingeniería Social aprovecha las tendencias naturales de una persona, confía en su habilidad de palabra, y combina estas técnicas con los agujeros de seguridad de los sistemas para lograr acceder a un sistema donde carece de permisos.

Subsubsección 1.2.4.1.- Motivación para un ataque de Ingeniería Social

Las motivaciones que puede tener una persona para querer realizar Ingeniería Social son múltiples y diversas. Entre estas, las más importantes son las siguientes, aunque no son las únicas:

1) **Ganancia financiera.-** Una persona puede estar atrapado en problemas económicos, o simplemente desea hacerse rico de manera fácil y rápida. Para lograr lo anterior, el practicante de la Ingeniería Social puede inculpar a alguien ajeno a sus intereses en una situación de robo de identidad o de fraude.

2) **Interés propio.-** Una persona puede, por ejemplo, querer acceder, obtener, usar y/o modificar información asociada consigo mismo, con un miembro familiar o amigos. Con ello puede buscar beneficiarlos o simplemente ganar tiempo para intentar cubrir sus rastros.

3) **Venganza.-** Por razones solo verdaderamente conocidas por una persona, puede convertir su objetivo en su amigo, colega u organización para satisfacer su deseo emocional de venganza.

4) **Presión externa.-** Una persona puede estar recibiendo presión por amigos, familia, u organizaciones del crimen organizado por razones tales como ganancia financiera, interés propio y/o venganza.

Subsubsección 1.2.4.2.- Fases de un Ataque de Ingeniería Social

Cada ataque de ingeniería social es único, con la posibilidad de que pueda incluir diversas fases o ciclos para alcanzar el resultado final deseado.

Comúnmente un ataque de Ingeniería social presenta las siguientes fases:

1) **Recopilación de información.-** Un atacante o delincuente puede utilizar diversas técnicas para recopilar información acerca de su objetivo o víctima. Una vez obtenida esta información puede ser usada para construir una relación con el objetivo o con alguien importante para el éxito del ataque.

Algunos ejemplos, (pero no limitados a estos) son los siguientes:

- Lista telefónica
- Fechas de cumpleaños
- Cuadros organizacionales de la empresa
- Información sobre hábitos y familia de la víctima

2) **Desarrollar una relación.-** Un atacante o delincuente puede libremente aprovechar el deseo de un objetivo o víctima de sentirse en confianza para desarrollar compenetración con ellos. Mientras se desarrolla esta relación, el atacante o delincuente puede ubicarse en una posición de confianza, de la cual más adelante se aprovechará. Algunos ejemplos, (pero no limitados a estos) son los siguientes:

- Demostrar intereses comunes
- Festejar cumpleaños
- Invitaciones a restaurantes o bares
- Halagos y obsequios

3) **Aprovechamiento.-** El objetivo o víctima puede entonces ser manipulado por el atacante o delincuente “confiable” para revelar información (por ejemplo claves o contraseñas) o realizar una acción que normalmente no ocurriría. Esta acción puede ser el final del ataque o el inicio de la siguiente fase. Algunos ejemplos, (pero no limitados a estos) son los siguientes:

- Revelar fechas (cumpleaños, nacimiento del primogénito, boda, etc.)
- Revelar nombres (esposo(a), hijo/a(s), mascotas, apodos, etc.)
- Revelar gustos (hobbys, programas de t.v., autos, etc.)

4) **Ejecución.-** Una vez que el objetivo o víctima ha completado la tarea requerida por el atacante o delincuente, el ciclo es completado con la obtención de la información.

Subsubsección 1.2.4.3.- Técnicas de Ingeniería Social mediante las cuales puede ser vulnerada la seguridad de un sistema

El éxito de las técnicas que pueden ser usadas se basan en la fuerza, habilidad y capacidad del practicante de la Ingeniería Social.

La primera fase de un ataque probablemente incluirá la recopilación de información acerca del objetivo o víctima.

Algunos ejemplos de las técnicas de recopilación de información que podrían ser usadas, son las siguientes:

1) **Observación desapercibida.-** Mirar sobre el hombro de un individuo mientras escribe o teclea su clave o contraseña de acceso (usuario y contraseña) en un teclado con el propósito de memorizarlo para, más tarde, poder reproducirlo y mediante éste poder acceder a elementos (sistemas de software, equipo de cómputo, programas, etc.) a los cuales no tiene permisos.

2) **Revisar la basura.-** Buscar en la basura para obtener información potencialmente útil que debería ser desechada de manera más segura. Comúnmente se desechan archivos, notas en papel, dispositivos de almacenamiento aparentemente inútiles que pueden tener información

personal o de la organización y ésta no tiene implementadas políticas de destrucción de estos archivos. Esto permite que incluso el personal de limpieza pueda encontrar información aprovechable.

3) **Correos.-** La información de un individuo u organización es recopilada incitándolo(a) a participar en encuestas que ofrecen incentivos, como premios por completar la encuesta, entre otros. Es común que los usuarios reciban correos indicándoles que alguno de sus programas está por ser actualizado por lo cual, para no perder su información de la base de datos, se le solicita la reingrese, inclusive mostrando elementos como imágenes de la organización a la que pertenece o del programa en cuestión para proporcionar una sensación de autenticidad. Incluso, se puede solicitar ingresar claves y contraseñas con el pretexto de revisarlas.

4) **Análisis forense.-** Obtener componentes de equipo de cómputo como discos duros, memorias, DVD/CD'S e intentar extraer información que pueda ser útil para un individuo u organización. Es común que los administradores del sistema tengan respaldos o guarden archivos que están actualizando, los cuales, pueden contener la información de sus usuarios incluyendo sus contraseñas. Esta información es indebidamente protegida y si alguna otra persona adquiriera este dispositivo de almacenamiento podría ver toda esa información, sin ningún problema. Hoy en día existen diversos programas ("keyloggers", ya detallados en la Subsección 1.2.1 de este Anexo Técnico) que, instalados en una memoria USB, se ejecutan cuando ésta es ingresada en una nueva computadora, obteniendo los usuarios y contraseñas que se han utilizado, los sitios visitados, entre otros, durante el tiempo que ha estado encendido el equipo de cómputo.

Después de finalizar esta fase (la cual es normalmente la más larga del ataque, desde la perspectiva del atacante) un atacante o delincuente puede usar una de diversas técnicas para lograr su objetivo final. Cada técnica puede ser agrupada en una de dos categorías. La primera categoría es “basada en el humano” y se basa en relaciones interpersonales, mientras que la segunda está “basada en equipo de cómputo” y recae en tecnología.

Sin importar la técnica usada, un practicante de la ingeniería social seguramente favorecerá la simplicidad para asegurar su éxito. Algunas técnicas comunes son las siguientes:

1) **Usuario importante.-** Pretendiendo ser una persona de alto rango dentro de la organización con una fecha límite importante, el atacante o delincuente podría presionar a otro individuo para revelar información, tal como:
   - El tipo de software de acceso remoto usado.
   - Cómo configurarlo.
   - Los datos técnicos que son necesarios para conectarse al servidor de acceso remoto.
   - Las contraseñas para registrarse en el servidor.

   Una vez obtenida esta información, el atacante o delincuente puede entonces establecer un acceso remoto a la red de la organización. El atacante o delincuente podría entonces llamar algunas horas más tarde para explicar que ha olvidado la clave de su cuenta y solicitar que sea reestablecido.

2) **Usuario desvalido.-** Un agresor puede pretender ser un usuario que requiere asistencia para obtener acceso a los sistemas de la organización. Este es un proceso simple de realizar por parte de un atacante o delincuente, particularmente si no ha sido capaz de obtener suficiente información acerca de la organización. Por ejemplo, el atacante o

delincuente podría llamar a una secretaria de la organización y pretender ser un nuevo usuario temporal el cual ha tenido problemas para accesar al sistema de la organización. No deseando ofender a la persona, o parecer incompetente, la secretaria puede sentirse inclinada a proporcionar el usuario y contraseña de una cuenta activa.

3) **Personal de soporte técnico.-** Pretendiendo pertenecer al equipo de soporte técnico de una organización, un atacante o delincuente podría extraer información útil de un usuario de manera que no sospeche nada.

   Por ejemplo, el atacante o delincuente podría pretender ser un administrador del sistema el cual intenta ayudar con un problema del sistema y requiere el usuario y clave para resolver el problema.

4) **Sitios web.-** Su objetivo es realizar una estafa o engaño para lograr que un usuario inconsciente o ignorante de los factores de seguridad revele información potencialmente sensitiva. Por ejemplo, un sitio web puede anunciar una promoción o competencia ficticia, la cual requiere que el usuario ingrese su correo para contactarlo y una contraseña. Esta clave ingresada será, la mayoría de las veces, el mismo o muy similar a la clave usada por el usuario en el trabajo.

5) **Phishing.-** Esta técnica utiliza emails que incitan a visitar algunos sitios web. Estos sitios probablemente sean diseñados, usando anuncios de marcas conocidas, para convencer al individuo que proporcione información personal o financiera. Esta información será usada para propósitos fraudulentos. En algunos casos, mientras se visita un sitio web, códigos maliciosos como “keyloggers” son instalados, sin que el usuario se dé cuenta, para obtener información sensible del individuo tales como claves o contraseñas.

Subsubsección 1.2.4.4.- Uso de Ingeniería Social para lograr tener acceso al Sistema de Software “AS” de la Institución Bancaria.

Debido a las diversas debilidades, documentadas en este reporte, que presenta el sistema e software “AS”, un atacante o delincuente podría apoyarse de estas técnicas de Ingeniería Social y con ello lograr adquirir la información sensible, como son las *claves* o *contraseñas* de los usuarios legítimos y autorizados, para realizar, con esta información, transacciones fraudulentas.

Obtener acceso al sistema, por parte de un atacante o delincuente, aplicando estas técnicas, es más sencillo para una persona familiarizada con dicho sistema o con el movimiento interno diario de la empresa contratante del sistema de software.

El hecho de que una persona haya pertenecido a la empresa (en este caso la Institución Bancaría) donde se encuentra instalado este sistema, hace que conozca el sistema mismo, conozca el lenguaje interno de la empresa, así como a los usuarios del sistema. Esto le hace más fácil entablar una relación para obtener información sensible. Debido a su conocimiento de instalaciones, funcionamiento interno, personas, horarios, que como ex empleado tiene, le hace más fácil burlar las medidas de seguridad, tanto físicas como del sistema de software.

Esta clase de técnicas de Ingeniería Social son continuamente utilizadas y debido a la falta de controles de seguridad suelen pasar desapercibidas para las empresas, por lo que su detección, si es que es detectada, generalmente sucede después de sufrir grandes pérdidas.

Sección 1.3: Vulnerabilidad al no asegurar la información que se intercambia durante la ejecución del Sistema de Software “AS” de la Institución Bancaria.

El intercambio de información entre dos o más equipos de cómputo utilizando una red (ya sea de uso dedicado o no) es susceptible de ser observada, capturada y hasta modificada por un atacante o delincuente, mediante la utilización de programas escucha, denominados “sniffers” (tratados con detalle en la Sección 1.2, Subsección 1.2.3, de este mismo Anexo Técnico), o mediante hardware dedicado para escuchar el medio por donde se transmite la información.

Esto es posible debido a que la información que viaja por el medio de transmisión en tales redes y sistemas de comunicación se intercambia “en claro”, es decir, sin cifrar. El cifrado es un mecanismo de seguridad que garantiza que la información que se transfiere por un canal de comunicaciones, aunque el atacante o delincuente, mediante cualquier medio, tenga acceso a ella, no sea entendida más que por las partes legítimamente autorizadas para entenderla.

El sistema de software “AS” permite que la información de todo tipo que se intercambia entre el programa cliente (instalado del lado de la empresa, en este caso sucursal) y el programa servidor (instalado del lado de la institución bancaria) tal como: *nombre de usuario*, *claves* o *contraseñas, montos de las transacciones, etc.,* viaje “en claro”. Por lo tanto, cualquier atacante o delincuente interesado en capturar esta información, usando cualquier método de los descritos en la Sección 1.3 de este mismo reporte de peritaje, pueda hacerlo y con ello poder realizar transacciones ilícitas.

El acceso a los recursos o servicios que presta el sistema ya mencionado se realiza mediante la previa autenticación o identificación por medio de clave o contraseña del usuario en cuestión. Si esta información es proporcionada y enviada a través de un medio no cifrado permite que algún usuario malintencionado sea capaz de obtener esta información y utilizarla para hacerse pasar por un usuario legítimo.

La información del usuario al registrarse así como también la información que confirma la autorización de una operación es capturada mediante un programa tipo “sniffer” (tratados con detalle en la Sección 1.2, Subsección 1.2.3, de este

mismo Anexo Técnico), los mecanismos de seguridad que posee el sistema de referencia (de por sí obsoletos) son totalmente vulnerados.

Para este tipo de sistema de software se deben implementar, de acuerdo a los estándares internacionales ISO 17799 e ISO 27001, mecanismos para garantizar que la información que está en tránsito garantice propiedades de seguridad tales como confidencialidad, autenticación e integridad.

El hecho de no cifrar la información en un sistema de software de este tipo está incluso penalizado en otros países. Esto debido a que no sólo se expone la cuenta bancaria y los correspondientes recursos de cada uno de los clientes de la Institución bancaria, sino también información personal importante de cada uno de ellos.

Sección 1.4.- Vulnerabilidad al no implementar autenticación mutua entre el cliente y el servidor previo a la ejecución del Sistema de Software “AS” de la Institución Bancaria.

El servicio de seguridad llamado autenticación consiste en que las dos partes involucradas en una comunicación se demuestren ser quienes dicen ser. La autenticación es unilateral, si sólo una de las dos partes demuestra ser quien dice ser, pero la otra parte no lo hace. Se dice que la autenticación es mutua cuando ambas partes se demuestran ser quienes dicen ser.

En el sistema de software “AS” la autenticación es unilateral y, además débil. Es unilateral porque sólo la entidad cliente (en este caso Sucursal bancaria) se autentica ante el servidor (en este caso Grupo Financiero) pero este último no demuestra ser quien dice ser al cliente. Es débil porque la autenticación está basada en algo que sabe (en este caso una *clave* o *contraseña* débil (tratado con detalle en la Sección 1.2 de este mismo Anexo Técnico)).

Es decir, el sistema de software “AS” no implementa autenticación mutua. La autenticación que implementa es unilateral y débil.

Lo anterior representa una vulnerabilidad grave del sistema ya que, a partir de ello, se presentan los siguientes escenarios de ataques reales los cuales vulneran al sistema y permiten suplantación de las partes legítimas y autorizadas para realizar transferencias fraudulentas:

1. Un atacante o delincuente puede levantar un sitio falso que, representando ilegítimamente al proceso servidor de la aplicación “AS”, se haga pasar por ella y capturar los datos sensibles (*nombre de usuario* y *clave o contraseña*) del proceso cliente de la misma aplicación “AS” y con ellos, posteriormente, establecer una comunicación por su cuenta con el banco (ya se mostró con detalle en las Sección 1.3 de este mismo Anexo Técnico que esto es posible) para, usurpando al proceso cliente (en este caso al cajero que lo opera), realizar transacciones fraudulentas como si se tratara del cajero legítimo.
2. La falta de autenticación mutua en este tipo de sistemas provoca el tipo de ataque conocido popularmente como “robo de identidad” y que resulta del escenario detallado en el punto 1 anterior.
3. La autenticación débil permite el tipo de ataques detallados en la Sección 1.2 de este mismo Anexo Técnico.

A continuación se presentara la tabla que resume las actividades realizadas en la fase de creación del reporte *(Véase tabla 5.28).*

Tabla 5.28 Etapas de la fase Creación del reporte.

Fase de Creación del reporte		
Preguntas claves	• ¿La información sirve para comprobar los resultados? ¿La información sirve para comprobar la integridad de los datos?	
Etapas	• Reporte de la fase de identificación	• Dentro del reporte se agrega una introducción nombrando los hallazgos que se tuvieron en la fase de identificación.
	• Reporte de la fase de adquisición de evidencia	• Para comprobar que la evidencia se encuentra integra se nombra como es que se tuvo acceso a las imágenes forenses. • Se nombran todas las fuentes a las que se tuvo acceso para poder realizar el análisis –fotos, videos, equipo de cómputo, etc-
	• Reporte de la fase de análisis	• Se reportan todos los resultados obtenidos durante la fase de análisis.
	• Dar respuesta a las interrogantes de las partes y de la autoridad.	• Se reportaron los resultados en el formato que el abogado solicito. Contestando a una serie de puntos expuestos.
	• Elaboración de conclusiones	• Se realizaron conclusiones con base en los resultados obtenidos de la investigación.
	• Validación con un abogado.	• Antes de presentar este dictamen ante la autoridad se valido con un abogado con el fin de no incluir respuestas de carácter interpretativo, persusaivo y/o legal.

8. Fase de Retroalimentación y devolución de evidencia.

Esta fase tiene como objetivo regresar a la entidad toda la información que proporcionó o asegurarle que se ha realizado el borrado seguro de esta en caso de que se trate de información digital.

Otro objetivo que se tiene dentro de esta fase es la realización de mejoras al sistema con base en los resultados obtenidos durante la investigación forense.

8.1. Retroalimentación.

En esta etapa se propone que los resultados obtenidos de la investigación forense sean utilizados para mejorar los controles, reglas y políticas de seguridad para fortalecer la seguridad del sistema y evitar que se vuelvan a presentar incidentes del mismo tipo.

Es posible hacer estas recomendaciones porque se cuenta con una información basta de cómo funciona el sistema y donde se encuentran sus principales debilidades, así como una teoría de que fue lo que se vio vulnerado para provocar el ataque que produjo daños al sistema.

En este caso como la investigación que se llevó a cabo fue por petición de la parte acusada, por lo cual no era factible llevar a cabo esta etapa de la metodología.

Sin embargo si se hubieran podido dar algunas recomendaciones para incrementar la seguridad del sistema, las cuales repercuten en la seguridad de los usuarios –clientes y trabajadores-.

A continuación se presentarán las recomendaciones derivadas de la investigación de cómputo forense.

8.1.1 Autenticación al sistema.

Se encontró que la autenticación al sistema que estaba implementada al momento del incidente era de un solo tipo –por algo que se sabe-. Era una autenticación por contraseña.

Además estas contraseñas eran débiles, ya que sólo constaban de 4 caracteres los cuales no necesariamente tenían que ser alfanuméricos ni mucho menos contar con símbolos especiales.

Por lo que se recomienda que estas sean construidas de manera correcta, capacitando al personal para que sepa construir una buena contraseña e implementando reglas en el código para que no permita que el usuario de alta una contraseña débil.

Así como llevar una buena administración de las contraseñas, ya que estas no deben de ser usadas por mucho tiempo.

- Para que una contraseña se considere fuerte debe de ser construida con ciertas características.
  - Longitud mínima
  - Uso de caracteres alfanuméricos y símbolos especiales.
  - No usar palabras del diccionario.
  - Tiempo de caducidad.

Longitud mínima.

La longitud mínima es de ocho caracteres. Considerando que la contraseña está bien construida es decir contiene caracteres alfanuméricos y caracteres especiales.

Caracteres alfanuméricos y símbolos especiales.

Con el fin de construir una contraseña fuerte se tienen que agregar a ella caracteres alfanuméricos y símbolos especiales, al hacerlo lo que estamos logrando es aumentar el número de posibles combinaciones que se pueden tener.

Esto es bueno ya que un ataque muy utilizado para descifrar contraseñas es el ataque de fuerza bruta, el cual prueba con diferentes combinaciones hasta que encontrar la contraseña. Si el número de combinaciones es más grande más tiempo tardará en probar todas ellas.

De esta manera si tenemos una contraseña que sólo use caracteres alfabéticos entonces tendremos la posibilidad de usar de la letra “a” a la “z” teniendo 27 posibles caracteres, suponiendo que la contraseña es de ocho caracteres entonces se tendrán 27^8 posibles combinaciones. Si aparte dentro de la contraseña metimos algunas letras mayúsculas entonces tendremos 27 caracteres más y las combinaciones van creciendo aumentando en este caso a 54^8.

Al agregar a nuestra contraseña números y símbolos especiales tenemos en total 108^8 posibles combinaciones.

Considerando que una computadora aproximadamente puede realizar cien millones de operaciones por segundo -10^8- entonces tenemos que se tardara $27^8/10^8$ tiempo en descifrar nuestra contraseña.

A continuación se muestra una tabla con los tiempos que se tardaría en ser rota una contraseña de 6, 7, 8 y 9 usando caracteres del alfabeto en minúsculas, minúsculas y mayúsculas y minúsculas, mayúsculas, números y símbolos especiales (Véase tabla 5.29).

Tabla 5.29 Tiempo aproximado para romper una contraseña.

Longitud	Minúsculas	Agregar Mayúsculas	Agregar Números y símbolos especiales
6 caracteres	4 segundos	4 minutos	2 horas
7 caracteres	2 minutos	4 horas	7 días
8 caracteres	47 minutos	8 días	2 años
9 caracteres	21 horas	1 año 3 meses	167 años

No usar palabras del diccionario.

El no usar palabras que puedan estar contenidas en un diccionario sirve para evitar ataques de diccionario. Los cuales prueban las diferentes palabras que contienen el diccionario para poder romper una contraseña.

Tiempo de caducidad.

El marcar un tiempo de caducidad a la contraseña sirve ya que si esta se toma para intentar romperla y el romperla les toma algunos meses. La información que resguarda esta contraseña volverá a estar segura porque ya se habrá realizado el cambio de contraseña.

Hay que recordar que cada vez el poder del cómputo crece, por lo tanto cada vez es poco el tiempo que se necesita para romper una contraseña.

Dentro de las reglas del sistema debería de marcarse un tiempo límite para usar esa contraseña y forzar al usuario a que la cambie.

Uso de biométricos.

La autenticación del personal para realizar movimientos bancarios debe ser una autenticación fuerte pues se tiene acceso a información sensible de los clientes.

Para lograr una autenticación robusta se puede implementar más de un tipo de autenticación. Existen tres tipos:

- Por algo que se sabe.
- Por algo que se tiene.
- Por algo que se es.

El uso de una contraseña para autenticarse entra en el tipo “por algo que se sabe”. El tipo que se propone implementar es el tercero aquí mencionado “por algo que se es” se propone este porque es difícil de falsificar, ya que se toman características inherentes a la persona como lo es su huella digital.

Para poder implementar este tipo de autenticación se hace uso de los mecanismos biométricos, los cuales leen características únicas de los individuos comparándolas con una base de datos cargada previamente. Si estos dos coinciden entonces permitirá el acceso de esa persona al sistema.

8.1.2 Autenticación mutua.

Se encontró una vulnerabilidad en el sistema al notar que para autenticarse ante el servidor se emplea una autenticación unilateral, es decir sólo una de las partes que intervienen en la comunicación se autentica.

En este caso sólo las terminales se autenticaban ante el servidor pero este no se autenticaba ante las terminales.

Este tiene grandes consecuencias pues quiere decir que es posible que las terminales estén recibiendo órdenes e información de alguien que no es quien dice ser.

Por lo cual se recomienda la implementación de una autenticación mutua, en la cual tanto las terminales como el servidor se autentiquen una ante la otra.

Este tipo de autenticación puede ser implementada con el uso de la firma digital, la cual proporciona autenticación de identidad y autenticación de origen de datos.

Firma digital.

En seguridad informática, un proceso de firma digital (ya sea de un mensaje o, en este caso, de una transacción) se realiza mediante una transformación matemática que depende del contenido, del mensaje o transacción en este caso, y de un factor de autenticación (una llave privada criptográficamente fuerte) que autentica al usuario como legítimo y que lo relaciona con la operación. Esta transformación es única y sólo puede ser realizada por la persona que relaciona la

operación con la llave privada. De esta forma la identidad de la persona queda relacionada con el proceso.

Además, en el concepto de firma digital, para validar la legitimidad de la operación, el verificador de tal operación debe poseer y usar para tal verificación, un certificado de llave pública expedido y firmado digitalmente por una Autoridad Certificadora confiable. La llave pública, que la aplicación extrae del Certificado Digital, una vez corroborada la validez del firmante que lo expide, está relacionada matemáticamente con la llave privada que el usuario legítimo usó para realizar la transacción. Si esta verificación de la firma es válida se acepta la transacción como legítima, es decir, como realizada realmente por el poseedor único de la llave privada, de lo contrario se rechaza.

Al no estar implementado este concepto de Firma Digital en el sistema de la institución lo hace susceptible a todos los riegos de suplantación de usuarios legítimos.

8.1.3 Integridad de bitácoras.

Al momento de analizar las imágenes forenses del sistema se encontró que las bitácoras del día en que ocurrió el incidente habían sido eliminadas. Por lo cual se recomienda que existan políticas para la eliminación de bitácoras, ya que estas contienen información muy importante para la institución bancaria.

No se puede permitir que cualquier persona tenga acceso a estos archivos y cuente con los permisos necesarios para realizar el borrado de estos.

Al analizar este sistema se pudo notar que estos archivos no contaban con ninguna restricción para ser borrados o modificados por cualquier usuario.

Para conservar la integridad de las bitácoras se recomienda que se administren los permisos de las carpetas que las contienen para que sólo aquellas

personas autorizadas y después de determinado tiempo puedan eliminar la información que en ellas se almacena.

Además de administrar los permisos de las carpetas estos archivos podrían ser almacenados de forma cifrada para evitar que alguna persona pudiera acceder a ellos para modificarlos. Al implementar el mecanismo de cifrado se garantiza el servicio de integridad.

Este tipo de información debe de contar con un tiempo de vida calculado previamente en el cual no pueden ser eliminadas ni por las personas que tengan autorización de hacerlo. Esto garantiza que se tenga la información en caso de que se requiera aclarar algún movimiento bancario hecho por cualquiera de los cajeros.

8.1.4 Acceso remoto.

Dentro del sistema se encontró que se operaban programas que permitían acceso remoto a otras computadoras las cuales podían hacer cambios y registrar actividades desde algún otro sitio.

Por lo cual se recomienda que se implemente una buena administración de este tipo de programas restringiendo el acceso sólo a aquellas computadoras que se encuentren autorizadas.

Para lo cual es necesario implementar un buen sistema de autenticación robusta.

8.2. Devolución de evidencia.

Todo analista forense se encuentra en la obligación de garantizar al cliente confidencial, con respecto al caso en proceso, al contenido de las actuaciones judiciales y al resultado de sus investigaciones.

También se encuentra obligado a proteger los datos personales del cliente entre otras.

Con el objetivo de cumplir con estas obligaciones es que se realiza esta etapa de devolución de evidencia, en la cual se propone realizar la eliminación de toda la evidencia digital después de haber terminado el caso. Así como hacer la devolución de la evidencia escrita que haya sido entregada al analista o forense o bien realizar la destrucción de esta.

Para realizar la eliminación de la evidencia digital se pueden implementar cualquiera de los siguientes métodos:

- Borrado seguro.
- Destrucción del medio físico
- Magnetización del medio físico.

Borrado seguro.

El borrado seguro se realiza usando herramientas especiales las cuales hacen una sobreescritura del medio físico varias veces.

Dependiendo de la herramienta usada será el algoritmo que use, se recomienda que se busque alguna herramienta que haga la sobreescritura del medio por mínimo siete veces. De lo contrario existen formas de recuperar la información.

Destrucción del medio físico.

Esta es otra técnica para eliminar la información contenida en un medio aunque no es tan recomendable ya que no sólo se pierde la información sino que el disco queda completamente inutilizable.

Para destruir el medio se puede quemarlo, perforarlo, comprimirlo…

Magnetización del medio.

Para poder llevar a cabo este método que permite realizar la eliminación de información digital de su medio se requiere imanes potentes que sean capaces de cambiar los bits de información que contiene el disco…

Pero si la información no se encuentra en ningún medio digital y se tiene escrita en papel entonces se puede llevar a cabo la trituración del papel, con el objetivo de eliminar la posibilidad de que sea accedida por personal no autorizado.

Eliminación de información escrita en papel.

En el caso de que lo que se desee eliminar será información que se encuentre escrita en papel se deberá hacer uso de trituradoras de papel, las cuales reducen las hojas de papel a pequeñas tiras o hasta a pequeñas bolitas parecidas al confeti.

A continuación se presentara la tabla que resume las actividades realizadas en la fase retroalimentación y devolución de evidencia. *(Véase tabla 5.30 y 5.31)*

Tabla 5.30 Resumen de la fase de retroalimentación y devolución de evidencia en la etapa de retroalimentación.

Fase de Retroalimentación y devolución de evidencia		
	Retroalimentación	
Preguntas claves	• ¿Cómo mejorar? • ¿Ha sido eliminada la evidencia?	
Etapas	• Exposición de resultados • Toma de decisiones	• Se plantean los problemas encontrados en el sistema. • Se proponen soluciones ante estos problemas.

Tabla 5.31 Resumen de la fase de retroalimentación y devolución de evidencia en la etapa de devolución de evidencia.

Fase de Retroalimentación y devolución de evidencia		
	Devolución de la evidencia	
Preguntas claves	• ¿Cómo mejorar? • ¿Ha sido eliminada la evidencia?	
Etapas	• Devolución de documentos • Borrado seguro • Trituración de información empresa	• Se hizo el borrado seguro de la información digital. • Se realizó la trituración de información escrita en papel.

Capítulo Sexto
Resultados y Conclusiones.

En este capítulo se expondrán los resultados y conclusiones del trabajo realizado. Dentro de los resultados se encontraran dos categorías los resultados obtenidos del análisis de las metodologías forenses y los resultados de la aplicación de la metodología a un caso práctico.

Así mismo se presentarán las conclusiones divididas en tres líneas rectoras: la necesidad de concientización del uso de medios digitales, los crímenes digitales, el cómputo forense y el procedimiento legal y por último las conclusiones del caso práctico.

1. Resultados.

Se obtienen dos resultados. El primero relacionado con el aporte de la metodología de cómputo forense y el segundo con los resultados obtenidos al emplear la metodología propuesta en un caso real de investigación.

1.1 Metodología de cómputo forense.

Después de realizar un análisis comparativo de las mejores metodologías en existencia se realizó la propuesta de una metodología de cómputo forense general.

Metodología que reunió las mejores propuestas de las metodologías analizadas, dio solución a los principales problemas que se encontraron en el análisis y propuso nuevas fases que dan respuesta a los retos forenses. Haciendo de esta, una metodología, no sólo aplicable dentro de una investigación de cómputo forense para ofrecer respuestas a la justicia, sino también como una herramienta para robustecer la seguridad de los sistemas.

Se logró que la metodología de cómputo forense fuera aplicable a cualquier tipo de dispositivo que almacene evidencia digital, sin importar el tipo de tecnología que utilice. Haciéndola útil para analizar cualquier dispositivo encontrado en la escena del crimen.

Debido a su estructura en la que marca por cada fase un objetivo, actividades específicas y herramientas que se pueden utilizar, hace que el tiempo invertido en la investigación se reduzca.

Los resultados obtenidos al seguir esta metodología pueden ser presentados en un proceso legal ya que durante el desarrollo de toda la investigación se cuida la integridad de la evidencia como parte fundamental del proceso.

1.2 Resultados del Caso práctico.

Se aplicó la metodología forense propuesta desarrollando una investigación de cómputo forense real, llevada a cabo en el Laboratorio de Seguridad Informática ubicado en la FES “Aragón”.

Al realizar la investigación forense siguiendo la metodología propuesta en este trabajo, se obtuvieron resultados que fueron presentados ante una corte legal, para que se pudiera dar un veredicto con respecto al caso.

Los resultados fueron reportados, con fundamentos en las evidencias encontradas en los sistemas bancarios, previamente preservados. También se entregó reporte de los procedimientos seguidos durante la investigación forense.

Los resultados que se obtuvieron del análisis del sistema bancario demuestran categóricamente que es imposible ligar a los inculpados con las actividades ilícitas registradas el día 2 de abril de 2008.

Después de hacer el análisis del sistema bancario, se pudieron detectar sus vulnerabilidades, por lo que es posible realizar recomendaciones que ayuden a mejorar la seguridad del sistema. Este tipo de acciones es importante si se desea mitigar el riesgo de nuevos incidentes.

2. Conclusiones.

Las conclusiones serán presentadas en tres líneas rectoras. La primera es la necesidad de concientización del uso de medios digitales, la segunda relacionada con los crímenes digitales, el Cómputo Forense y el procedimiento legal, por último las conclusiones obtenidas del análisis del sistema bancario.

2.1 Medios digitales.

El crecimiento acelerado de las herramientas tecnológicas y de los dispositivos de comunicación han provocado nuevos modelos de educación, entretenimiento, trabajo, comercio, e incluso ha cambiado el modelo para cometer delitos.

Los usuarios de estas tecnologías han aprendido con gran facilidad a desenvolverse en este nuevo esquema, en el cual se comunican, comparten información, manejan dinero, etc. Todo esto sin el menor recato.

Este cambio ha sido tan rápido que los usuarios tienen poca conciencia e información del tipo de riesgos que corren al usar de manera irresponsable las tecnologías.

Y no sólo son los usuarios finales los que cometen este error sino las personas que se dedican al desarrollo de sistemas, las cuales pocas veces se preocupan por implementar seguridad, sin mencionar que muchas veces la implementación se hace de manera incorrecta.

Este escenario proporciona las condiciones ideales a los criminales para realizar actividades ilícitas a gran escala. Esta es una de las razones por las que cada año se registra un aumento en el número de crímenes digitales en el mundo.

Se debe de entender que la seguridad no sólo es la aplicación de antivirus en una computadora. La seguridad es un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos, ante cualquier amenaza, preservando los servicios de autenticidad, confidencialidad, integridad y disponibilidad.

La importancia de implementar seguridad en los sistemas ya no es sólo para lograr la protección de la información, sino para evitar caer en un delito, pues ahora existen leyes que obligan a las personas encargadas de procesar o almacenar información sensible, a contar con seguridad en sus sistemas.

2.2 Crímenes digitales, cómputo forense y procedimiento legal.

Es indiscutible que el modelo para cometer crímenes ha cambiado, en este nuevo modelo las tecnologías forman parte fundamental, por lo que es necesario contar con expertos en la materia que ayuden a investigarlas y con un modelo legal capaz de legislarlas.

Sin embargo el comportamiento de crecimiento continuo y acelerado que poseen la tecnología, se vuelve un problema para el derecho que tiene que regular una materia que se encuentra en constante desarrollo, esto sin mencionar que las tradicionales normas jurídicas requieren de largos y complicados procesos. Es por esto que se ve casi inalcanzable el poder responder al reto.

A pesar de estas dificultades, la aplicación de metodologías forenses en las investigaciones de crímenes digitales, puede ser de gran ayuda siempre y cuando estas respondan a los principales retos del cómputo forense y lo hagan en el menor tiempo posible.

2.3 Conclusiones del análisis del sistema bancario.

Según cifras presentadas por la Comisión Nacional para la Defensa de los Usuarios de las Instituciones Financieras (Condusef) revelan que en el 2010 los fraudes bancarios provocaron que las entidades financieras del país, presentaran pérdidas por hasta 476 millones de pesos, panorama que según los expertos se podría mantener e incluso incrementar para el 2012.

Al analizar el sistema operado en la institución bancaria, se pudo detectar un problema que es común en muchos de los sistemas que se encuentran actualmente operando, éste es la falta de mecanismos y políticas de seguridad dentro de los sistemas.

Este problema provoca que las vulnerabilidades crezcan y las oportunidades de tener éxito en un ataque aumenten. Es por eso que se hace hincapié, en la necesidad de expertos en seguridad que sean capaces de mitigar los riesgos, así como de la concientización del personal que operara el sistema y de los usuarios finales.

La falta de procedimientos para dar respuesta ante un incidente provoca la pérdida de evidencia que lleve a identificar el tipo de ataque, su procedencia y su actor.

Aunque las instituciones bancarias presentan cientos de casos relacionados con fraudes financieros, éstas no cuentan con políticas y mecanismos de seguridad; por lo que al presentar un incidente de seguridad no saben cómo tratarlo y mucho menos como resolverlo.

Bibliografía consultada.

[Aguirre - 2006] Ramio Aguirre Jorge (2006). *Libro electrónico ce seguridad informática y criptografía [en línea] Versión 4.1 (6ta edición).* España: Escuela universitaria de informática de la universidad politécnica de Madrid. <http:criptored.upm.es/guiateoria/gt_m001a.htm> [consultada 26/06/2012]

Altheide Cory, Carvey Harlan (2011). *Digital Forensics with Open Tools*. Massachusetts: Elsevier Inc.

Asamblea Legislativa Del Distrito Federal, IV (2002). Legislatura. *Código Penal para el Distrito Federal.* Publicado en la Gaceta Oficial del Distrito Federal.

Brown Cristopher L. T. (2006). *Computer Evidence Collection and Preservation*. Massechusetts: Charles River Media,Inc.

Cámara de Diputados del H. Congreso de la Unión (1996). *Ley Federal del Derecho de Autor.* Publicada en el Diario Oficial de la Federación.

Cano M. Jeimy J (2009). *Computación forense. Descubriendo los rastros informáticos*. México D.F.: Alfaomega.

Carrier Brian (2005). *File System Forensic Analysis.* E.U.A: Addison Wesley Professional.

Carvey Arlan (2007). *Perl Scripting for Windows Security: Live Response, Forensic Analysis and Monitoring*. Massachusetts: Syngress.

Casey Eoghan (2010). *Handbook of Digital Forensics and Investigation*. California: Elservier Inc.

Galvin Silberschartz (1999). *Sistemas Operativos (5ta edición).* México: Pearson

Gomez Vieites Alvaro (2007). *Enciclopedia de la seguridad informática*. México D.F.: Alfaomega Ra-Ma.

Kahn, David (1974). *The codebreakers- the story of secret writing*. Inglaterra: Weidenfeld and Nicolson.

Kanagasinham Prathaben (2008). *SANS Institute InfoSec Reading Room: Data Lost Prevention.* (paper).

Kent Karen, Chevalier Suzanne, Grance Tim, Dang Hung (2006). *Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute and Technology*. Montgomery: Department of commerce United States of America.

Kleiman Dave, Cardwell Kevin, Clinton Timothy, Cross Michael, Gregg Michael, Varsalone Jesse, Wright Craig (2007). *The Official CHFI for Computer Hacking Forensics Investigator.* Massachusetts: Syngress.

Laboratorio de desarrollo IBM (1989). *OS/2 Manual de programación*. Madrid: McGraw Hill.

McClure Stuart, Scambrar Joel, Kurtz George (2009). *Hacking Exposed 6: Network Security Secrets & Solutions*. E.U.A.: McGraw-Hill.

Maiorano Ariel H (2009). *Criptografía. Técnicas de desarrollo para profesionales*. Paraguay: Alfaomega Grupo Editor Argentino.

Mandia Kevin, Prosise Chris, Pepe Matt (2003). *Incident Response and Computer Forensics (2da Edición).* E.U.A.: McGraw-Hill.

[Menezes y Van - 2001] Menezes Alfred J., Van Oorschot Paul, Vanstone Scott A (2001). *Handbook of Applied Cryptography*, E.U.A.: CRC Press 5ta ed.

Mohay George, Anderson Alison, Collie Byron, Del Vel Oliver, McKemmish Rod (2003). *Computer and Intrusion Forensics*. Massachusetts: Artech House.

Muñoz Torres Ivonne (2009). *Delitos Informáticos. Diez años después.* México D.F.: Ubijus.

Nolan Richard, O'Sullivan Colin, Branson Jake, Waits Cal (2005). *First Responders Guide to Computer Forensics*. Pittsburgh: Carnegie Mellon Software Engineering Institute.

Office of Justice Programs World Wide Web Site, National Institude of Justice World Wide Web Site (2001). *Electronic Crime Scene Investigation: A Guide for First Responders.* E.U.A: U.S Department of justice, Office of Justice Programs, National Institute of justice.

[Peltier 2005] Peltier R. Thomas (2005). *Information Security Risk Analysis*. Florida: Auerbach Publications. 325-2005

Philipp Aaron, Cowen David, Davis Chris (2010). *Hacking Exposed: Computer forensics.* E.U.A.: McGraw-Hill.

Picouto Ramos Fernando (2007), Lorente Pérez Iñaki, García Moran Jean Paul, Ramos Varón Antonio Ángel. *Hacking y Seguridad en Internet.* México D.F.: Alfaomega Ra-Ma.

Reyes Antony, Wiles Jack. *The Best Damn Cybercrime and Digital Forensics Period*. Massachusetts: Elversier Inc.

Scientific Working Group on Digital Evidence -SWGDE- (2006). *Best practices for Computer Forensics*. E.U.A.: SWGDE.

Singhal Anoop, Winograd Theodore, Scarfone Karen (2007). *Guide to Secure Web Services: Recommendations of the National Institute of Standard and Technology*. E.U.A.: U.S. Department of Commerce.

Tanenbaum Andew S., Woodhull Albert S. (1997), *Sistemas Operativos: Diseño e implementación (2da edición).* México: Prentice Hall

US-CERT (2008) *Computer Forensics*. US-CERT.

Vacca John R (2005). *Computer Forensics: Computer Crime Scene Investigation*. Massachusetts: Charles River Media.

William Stallings (1997). *Sistemas Operativos.* Madrid: Prentice Hall.

Zuccardi Giovanni, Gutiérrez Juan David (2006). *Informática Forense.* (paper).

Corella Frenandez Fidel, Venegas Toledo Manuel José, Viciano Blasco Guillermo (1999). *Seguridad y Control.* Última visita el 26 de junio de 2012. http://www4.uji.es/~al024444/conceptosbasicos.html

Norton by Symantec (2012). *Informe sobre Cibercrimen de Norton*. Última visita el 29 de enero de 2012 http://www.symantec.com/content/es/mx/home_homeoffice/html/cybercrimereport/

Olvera Carlos (2011). *Tipos de Computadoras y Más Allá: Estructura lógica de un Disco Duro (Cilindros, Cabezas, Sectores, Pistas, Cluster…).* Última visita *el 8 de Marzo de 2012.* http://tiposdecomputadora.wordpress.com/2011/05/23/estructura-logica-de-un-disco-duro-cilindros-cabezas-sectores-pistas-cluster%E2%80%A6/

Olvera Carlos (2012). *Tipos de Computadoras y Más Allá. Última visita el 25 de junio de 2012* http://tiposdecomputadora.files.wordpress.com/2010/12/asciicompleto.png

Anexo.

1) Dictaminar si el Sistema de Software denominado "AS" de la institución bancaria tiene las fortalezas de seguridad suficientes para prevenir y evitar transferencias de fondos por parte de personas no autorizadas.

Respuesta:

El sistema de Software denominado "AS" de la institución bancaria NO tenía, a la fecha de los hechos, las fortalezas de seguridad suficientes para prevenir y evitar transferencias de fondos por parte de personas no autorizadas.

Las razones son, entre otras, las siguientes:

1) De acuerdo a la información y a los diagramas del sistema "AS" que la institución bancaria proporcionó al perito, el procedimiento o protocolo de autenticación o identificación (servicio de seguridad mediante el cual una entidad o persona, por ejemplo el proceso cliente de la aplicación "AS", iniciado en este caso por la cajera principal, debe demostrar incontrovertiblemente a otra entidad o persona, en este caso el proceso servidor del aplicativo "AS", ser quien dice ser) es un procedimiento o protocolo totalmente débil en términos de seguridad. Es débil porque el elemento que sirve como autenticador consiste de una clave o contraseña débil, adivinable y rompible. Una contraseña o clave se dice que es débil cuando el número y tipo de caracteres que lo integran es pequeño. En el caso del aplicativo "AS", el número de caracteres de la contraseña es de 4 y su tipo es de caracteres alfabéticos y numéricos. El tiempo de ruptura o adivinación de una contraseña así conformada es del orden de unos cuantos segundos.

   Información detallada sobre estas debilidades se describen en la Sección 1.1 y en la Sección 1.2 del Anexo Técnico correspondiente a este Reporte de Peritaje.

2) El sistema de software denominado “AS” de la institución bancaria basa la autenticación o identificación del cajero y del funcionario o funcionarios, que autorizan eventualmente las transacciones, en ingresar al sistema una contraseña o clave para validar, y pretender demostrar con ello, la identidad del cajero o funcionario. No existe fundamento, ni técnico, ni científico, ni teórico, ni práctico, para relacionar la identidad de una persona con una contraseña o clave. El poseer una contraseña o clave nada tiene que ver con la identidad real de quien la posee. El que la posee o conoce, en un momento dado, puede ser una persona o proceso totalmente distinto de la persona o proceso que autorizadamente debiera poseerla y conocerla.

   Lo anterior se debe a que una contraseña o clave no es un elemento inherente a la naturaleza física y biológica del que la posee como, por ejemplo, sí lo son el DNA o la huella dactilar.

   Una contraseña puede ser robada, puede ser adivinada, puede ser expresamente rota con programas de cómputo, puede ser conocida por los administradores de un sistema como el denominado “AS” de la institución bancaria, puede ser conocida durante su viaje por el canal de red con programas de cómputo. Y una vez que una entidad, persona o proceso logra conocerla, puede hacer con ella lo mismo que hace la legítima poseedora de la misma. Por ejemplo, entre otras cosas, puede realizar operaciones y transferencias como si fuera la legítima poseedora.

   Un sistema que base la identificación de una persona en una contraseña o clave no puede, ni debe, pretender demostrar la

realización de un hecho con esa persona, con el argumento de que ese hecho se realizó con la contraseña que esa persona conocía. Eso no tiene sentido, ni justificación técnica ni científica.

Lo más parecido, en sistemas de identificación y autenticación, a la identificación real biológica es la utilización de autenticadores biométricos o lo que se conoce como firma digital. Ninguno de estos conceptos y autenticadores están implementados en el sistema denominado “AS” de la institución bancaria.

Información detallada sobre estas debilidades se describen en la Sección 1.1 del Anexo Técnico correspondiente a este Reporte de Peritaje.

3) El protocolo de autenticación o identificación del proceso cliente ante el proceso servidor del aplicativo “AS” también es débil porque, para autenticarse o identificarse ante el servidor, el proceso cliente debe revelar la contraseña. Siendo así, el mismo proceso servidor puede suplantar al proceso cliente.

   Información detallada sobre estas debilidades se describen en la Sección 1.1 y en la Sección 1.2 del Anexo Técnico correspondiente a este Reporte de Peritaje.

4) El protocolo de autenticación o identificación del proceso cliente ante el proceso servidor del aplicativo “AS” también es débil porque es unilateral. Es decir, el cliente se pretende autenticar ante el servidor pero el servidor no lo hace ante el cliente, razón por la cual el proceso servidor del aplicativo “AS” es suplantable por una persona o por otro proceso malicioso.

Información detallada sobre estas debilidades se describen en la Sección 1.4 del Anexo Técnico correspondiente a este Reporte de Peritaje.

5) El protocolo de autenticación o identificación del proceso cliente ante el proceso servidor del aplicativo “AS” también es débil porque, una vez que la contraseña de acceso se digita (teclea) y se le da entrada al sistema, la contraseña o clave autenticador viaja en claro por la red (de acuerdo al diagrama del aplicativo entregado por la institución bancaria al perito) y cualquier proceso o persona que monitoree el canal de red (por ejemplo un programa de software, de los conocidos como “sniffers”, o con un programa de software, de los conocidos como monitores de red, puede conocer sin problemas esa contraseña o clave y con ella suplantar a la persona dueña de esa contraseña o clave y realizar transacciones que en las bitácoras del sistema “AS” se verán como realizadas por el legítimo poseedor de tal contraseña o clave.

   Información detallada sobre estas debilidades se describen en la Sección 1.3 del Anexo Técnico correspondiente a este Reporte de Peritaje.

6) El protocolo de autenticación o identificación del proceso cliente ante el proceso servidor del aplicativo “AS” también es débil porque no tiene ninguna protección contra programas o dispositivos de los llamados “keyloggers”. Estos programas o dispositivos se utilizan para recolectar, sin que la persona o personas que utilizan un sistema de software se den cuenta de ello, datos o información sensibles, tales como claves o contraseñas. Estos programas existen en el mercado, a muy bajo precio, tanto en software como en hardware y pueden ser instalados fácil e imperceptiblemente (por

ejemplo como formando parte de un teclado de computadora), por personas con conocimientos básicos de cómputo.

Lo anterior se detalla en el Anexo Técnico en la sección 1.2, subsección 1.2.2.

2) Dictaminar si el Sistema de Software denominado "AS" de la institución bancaria tiene los huecos o vulnerabilidades de seguridad suficientes para permitir el robo y uso inadvertido de claves para realizar transferencias electrónicas por parte de personas no autorizadas.

Respuesta:

El sistema de Software denominado "AS" de la institución bancaria SÍ tenía, a la fecha de los hechos, los huecos o vulnerabilidades de seguridad suficientes para permitir el robo y uso inadvertido de claves para realizar operaciones electrónicas por parte de personas no autorizadas.

Las principales vulnerabilidades o huecos de seguridad, la mayoría de ellos ya mencionados y explicados en la respuesta a la pregunta 1, que el sistema de Software denominado "AS" de la institución bancaria tenía a la fecha de los hechos, son los siguientes:

1) El procedimiento o protocolo de autenticación es débil porque se basa en el uso de una contraseña o clave (además débil) para demostrar identidad de la persona que ingresa o utiliza el sistema.

   Información detallada sobre esta debilidad se describe en la Sección 1.1 y en la Sección 1.2 del Anexo Técnico correspondiente a este Reporte de Peritaje.

2) La contraseña o clave que usa el aplicativo “AS” es débil porque el número de caracteres de la contraseña es de 4 y su tipo es de caracteres alfabéticos y numéricos. El tiempo de ruptura o adivinación de una contraseña así conformada es del orden de unos cuantos segundos.

   Información detallada sobre esta debilidad se describe en la Sección 1.2 del Anexo Técnico correspondiente a este Reporte de Peritaje.

3) Una vez que la contraseña o clave de acceso se digita (teclea) y se le da entrada al sistema, la contraseña o clave viaja en claro por la red (de acuerdo al diagrama del aplicativo entregado por la institución bancaria al perito) y cualquier proceso o persona que monitoree el canal de red, por ejemplo un programa de software, de los conocidos como “sniffers”, o con un programa de software, de los conocidos como monitores de red, puede conocer sin problemas esa contraseña o clave y con ella suplantar a la persona dueña de esa contraseña o clave y realizar transacciones que en las bitácoras del sistema “AS” se verán como realizadas por el legítimo poseedor de tal contraseña o clave.

   Información detallada sobre esta debilidad se describe en la Sección 1.3 del Anexo Técnico correspondiente a este Reporte de Peritaje.

4) Una contraseña o clave puede ser robada, puede ser adivinada, puede ser expresamente rota con programas de cómputo, puede ser conocida por los administradores de un sistema como el denominado “AS” de la institución bancaria, puede ser conocida durante su viaje por el canal de red con programas de cómputo. Y una vez que una entidad, persona o proceso logra conocerla, puede hacer con ella lo mismo que hace la legítima poseedora de la misma. Por ejemplo, entre otras cosas, puede

realizar operaciones y transferencias como si fuera la legítima poseedora.

Información detallada sobre estas debilidades se describen en la Sección 1.2 y en la Sección 1.3 del Anexo Técnico correspondiente a este Reporte de Peritaje.

5) El sistema de software denominado “AS” de la institución bancaria basa la autenticación o identificación del cajero y del funcionario o funcionarios, que autorizan eventualmente las transacciones, en ingresar al sistema una contraseña o clave para validar, y pretender demostrar con ello, la identidad del cajero o funcionario. No existe fundamento, ni técnico, ni científico, ni teórico, ni práctico, para relacionar la identidad de una persona con una contraseña o clave. El poseer una contraseña o clave nada tiene que ver con la identidad real de quien la posee. El que la posee o conoce, en un momento dado, puede ser una persona o proceso totalmente distinto de la persona o proceso que autorizadamente debiera poseerla y conocerla.

   Información detallada sobre esta debilidad se describe en la Sección 1.1 del Anexo Técnico correspondiente a este Reporte de Peritaje.

6) El protocolo de autenticación o identificación del proceso cliente ante el proceso servidor del aplicativo “AS” no tiene ninguna protección contra programas o dispositivos de los llamados “keyloggers”. Estos programas o dispositivos se utilizan para recolectar, sin que la persona o personas que utilizan un sistema de software se den cuenta de ello, datos o información sensibles, tales como claves o contraseñas. Estos programas existen en el mercado, a muy bajo precio, tanto en software como en hardware y pueden ser instalados fácil e imperceptiblemente

(por ejemplo como formando parte de un teclado de computadora), por personas con conocimientos básicos de cómputo.

Información detallada sobre esta debilidad se describe en la Sección 1.2 del Anexo Técnico correspondiente a este Reporte de Peritaje.

7) El sistema de software denominado “AS” de la institución bancaria es vulnerable a la instalación de todo tipo de código malicioso, conocido genéricamente como “malware”, por parte de cualquier persona con acceso físico o lógico a los equipos de cómputo o al sistema de software. Los equipos donde residen los procesos cliente y servidor del aplicativo “AS”, de acuerdo al diagrama de ubicación mostrado, no están segregados y no tienen implementados controles de acceso que impidan que cualquier persona que ingresa a esa área (de acuerdo a la inspección física que realizó el perito y al diagrama que muestra el mapa de ubicación de esa área, las personas con acceso al área son al menos 4 cajeros, 2 subgerentes y demás funcionarios de la institución bancaria), pueda manipularlos o instalar aplicaciones de software o dispositivos de hardware maliciosos tales como “malware” o “keyloggers”.

   Información detallada sobre esta debilidad se describe en la Sección 1.2 del Anexo Técnico correspondiente a este Reporte de Peritaje.

3) Dictaminar si los controles de seguridad del Sistema de Software antes mencionado y de las propias instalaciones de la institución bancaria, lugar físico desde el cual se operó el mencionado sistema de software, cumplen con las recomendaciones de seguridad que exigen los estándares internacionales tales como el ISO 17799 y el ISO 27001.

Respuesta:

Los controles de seguridad del Sistema de Software antes mencionado y de las propias instalaciones de la institución bancaria y de su sucursal desde donde presuntamente se operó el mencionado sistema de software, NO cumplían, a la fecha de los hechos, con las recomendaciones de seguridad que exigen los estándares nacionales e internacionales, tales como el ISO 17799 y el ISO 27001.

Los controles de seguridad del Sistema de Software antes mencionado y de las propias instalaciones de la institución bancaria y de su sucursal. No cumplen con las recomendaciones de seguridad nacionales e internacionales, tales como los estándares ISO/IEC 17799:2005 e ISO 27001.

Sólo a manera de ejemplo de no cumplimiento con las recomendaciones de seguridad descritas en tales estándares de seguridad, a continuación se describen algunas de estas recomendaciones **incumplidas**:

De acuerdo al estándar ISO/IEC 17799:2005, respecto al Código de Prácticas para la administración de la seguridad de la información, las recomendaciones hechas por el estándar en los Capítulos siguientes, con sus correspondientes apartados, **no se cumplen:**

Capítulo 10.- Administración de Comunicaciones y Operaciones

10.2 Seguridad en los sistemas de aplicación

Objetivo: Prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación.

Se deben diseñar en los sistemas de aplicación, incluyendo las aplicaciones realizadas por el usuario, controles apropiados y pistas de auditoría o registros de actividad. Esto debe incluir la validación de datos de entrada, procesamiento interno y salida de datos.

10.2.3 Autenticación de mensajes

La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados en el contenido de un mensaje transmitido electrónicamente, o para detectar alteraciones en el mismo.

Puede implementarse en hardware o software que soporte un dispositivo físico de autenticación de mensajes o un algoritmo de software.

Se debe tener en cuenta la autenticación de mensajes para aplicaciones en las cuales exista un requerimiento de seguridad para proteger la integridad del contenido del mensaje, por ej., transferencias electrónicas de fondos u otros intercambios electrónicos de datos similares. Se debe llevar a cabo una evaluación de riesgos de seguridad para determinar si se requiere una autenticación de mensajes y para identificar el método de implementación más adecuado.

La autenticación de mensajes no está diseñada para proteger el contenido de un mensaje contra su divulgación no autorizada. Pueden utilizarse técnicas criptográficas como un medio adecuado de implementación de la autenticación de mensajes

10.2.4 validación de los datos de salida

La salida de datos de un sistema de aplicación debe ser validada para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias. Normalmente, los sistemas se construyen suponiendo que si se ha llevado a cabo una validación, verificación y prueba apropiada, la salida siempre será correcta. Esto no siempre se cumple. La validación de salidas puede incluir:

a) comprobaciones de la razonabilidad para probar si los datos de salida son plausibles;

b) control de conciliación de cuentas para asegurar el procesamiento de todos los datos;

c) provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente, determine la exactitud, totalidad, precisión y clasificación de la información;

d) procedimientos para responder a las pruebas de validación de salidas;

e) definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

10.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información. Deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

10.3.1 Política de utilización de controles criptográficos.

Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que tipo de control debe aplicarse y con qué propósito, y los procesos de la empresa.

Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, y para evitar un uso inadecuado o incorrecto. Al desarrollar una política se debe considerar lo siguiente:

a) el enfoque gerencial respecto del uso de controles criptográficos en toda la organización, con inclusión de los principios generales según los cuales debe protegerse la información de la empresa;

b) el enfoque respecto de la administración de claves, con inclusión de los métodos para administrar la recuperación de la información cifrada en caso de pérdida, compromiso o daño de las claves;

c) funciones y responsabilidades, por ej. quien es responsable de:

    1) la implementación de la política;

    2) la administración de las claves;

d) como se determinara el nivel apropiado de protección criptográfica;

e) los estándares que han de adoptarse para la eficaz implementación en toda la organización (que solución se aplica para cada uno de los procesos de negocio).

10.3.2 Cifrado

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se debe tener en cuenta para la protección de información sensible o critica.

Mediante una evaluación de riesgos se debe identificar el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la política de la organización en materia criptográfica, se deben considerar las normas y restricciones nacionales que podrían aplicarse al uso de técnicas criptográficas, en diferentes partes del mundo, y las cuestiones relativas al flujo de información cifrada a través de las fronteras. Asimismo, se deben considerar los controles aplicables a la exportación e importación de tecnología criptográfica.

Se debe procurar asesoramiento especializado para identificar el nivel apropiado de protección, a fin de seleccionar productos adecuados que suministren la protección requerida, y la implementación de un sistema seguro de administración de claves (ver también 10.3.5). Asimismo, podría resultar necesario obtener asesoramiento jurídico con respecto a las leyes y normas que podrían

aplicarse al uso del cifrado que intenta realizar la organización.

10.3.5 Administración de claves

10.3.5.2 Normas, procedimientos y métodos

Un sistema de administración de claves debe estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) generar y obtener certificados de clave pública;

c) distribuir claves a los usuarios que corresponda, incluyendo como deben activarse las claves cuando se reciben;

d) almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados;

e) cambiar o actualizar claves incluyendo reglas sobre cuándo y cómo deben cambiarse las claves;

f) ocuparse de las claves comprometidas;

g) revocar claves incluyendo como deben retirarse o desactivarse las mismas, por ej. cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deben archivarse);

h) recuperar claves pérdidas o alteradas como parte de la administración de la continuidad del negocio, por ej. la recuperación de la información cifrada;

i) archivar claves, por ej. , para la información archivada o resguardada;

j) destruir claves;

k) registrar (logging) y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves deben tener fechas de entrada en vigencia y de fin de vigencia, definidas de manera que solo puedan ser utilizadas por un periodo limitado de tiempo. Este periodo debe definirse según el riesgo percibido y las circunstancias bajo las cuales se aplica el control criptográfico.

Podría resultar necesario considerar procedimientos para administrar requerimientos legales de acceso a claves criptográficas, por ejemplo puede resultar necesario poner a disposición la información cifrada en una forma clara, como evidencia en un caso judicial.

Además de la administración segura de las claves secretas y privadas, también debe tenerse en cuenta la protección de las claves públicas. Existe la amenaza de que una persona falsifique una firma digital reemplazando la clave pública de un usuario con su propia clave. Este problema es abordado mediante el uso de un certificado de clave pública. Estos certificados deben generarse en una forma que vincule de manera única la información relativa al propietario del par de claves publica/privada con la clave pública. En consecuencia es importante que el proceso de administración que genera estos certificados sea confiable. Normalmente, este proceso es llevado a cabo por una autoridad de certificación, la cual debe residir en una organización reconocida, con adecuados controles y procedimientos implementados, para ofrecer el nivel de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicios o contratos con proveedores externos de servicios criptográficos, por ejemplo con una autoridad de certificación, deben comprender los tópicos de responsabilidad legal, confiabilidad del servicio y tiempos de respuesta para la prestación de los mismos

10.4 Protección contra código malicioso y móvil

Objetivo: Proteger la integridad del software y la información

10.4.1 Controles en contra de código malicioso

Control recomendado: *Deben implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso y procedimientos apropiados para la toma de conciencia de los usuarios*

10.5 Seguridad de los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.

Se deben controlar estrictamente los entornos de los proyectos y el soporte a los mismos.

Los gerentes responsables de los sistemas de aplicación también deben ser responsables de la seguridad del ambiente del proyecto y del soporte. Los gerentes deben garantizar que todos los cambios propuestos para el sistema sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema o del ambiente operativo.

10.5.5 Desarrollo externo de software

Cuando se realiza por medio de un tercero el desarrollo de software, se deben considerar los siguientes puntos:

a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual;

b) certificación de la calidad y precisión del trabajo llevado a cabo;

c) acuerdos de custodia en caso de quiebra de la tercera parte;

d) derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado;

e) requerimientos contractuales con respecto a la calidad del código; realización de pruebas previas a la instalación para detectar códigos troyanos.

10.7 Manejo de medios

Objetivo: Prevenir revelación no autorizada, modificación, eliminación o destrucción de activos, así como interrupción de las actividades del negocio

10.7.1 Manejo de medios removibles.

Control recomendado: debe haber procedimientos para la administración de medios removibles.

Capítulo 12.- Adquisición de Sistemas de Información desarrollo y mantenimiento

12.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información mediante medios criptográficos

12.3.1 Políticas en el uso de controles criptográficos

Control recomendado*: Debe desarrollarse e implementarse una política en el uso de controles criptográficos para la protección de la información.*

12.3.2 Administración de claves o contraseñas

Control recomendado: *Una administración de llaves debe ser ubicada para dar soporte a la organización acerca de las técnicas criptográficas.*

12.6 Administración de vulnerabilidades técnicas

Objetivo: *Reducir riesgos resultantes del aprovechamiento de vulnerabilidades técnicas publicadas.*

12.6.1 Control de vulnerabilidades técnicas

Control recomendado*: debe obtenerse oportunamente información sobre vulnerabilidades técnicas de los sistemas de información usados, evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar medidas apropiadas para asumir el riesgo asociado*

Las anteriores son sólo algunas de las múltiples recomendaciones del estándar internacional de seguridad ISO/IEC 17799:2005 que no se cumplen.

4) **Dictaminar si personas con conocimientos en cómputo, software, redes y sistemas computacionales pueden o no vulnerar las medidas de seguridad implementadas en el Sistema de Software denominado "AS" y utilizarlo inadvertidamente para fines fraudulentos.**

Respuesta:

Sí, en efecto, personas con conocimientos en cómputo, software, redes y sistemas computacionales podían, a la fecha de los hechos, vulnerar las medidas de seguridad implementadas en el Sistema de Software denominado "AS" de la institución bancaria y utilizarlo inadvertidamente para fines fraudulentos.

No sólo eso, personas con conocimientos mínimos y básicos en cómputo, software, redes y sistemas computacionales podían, a la fecha de los hechos, vulnerar las medidas de seguridad implementadas en el Sistema de Software denominado "AS" de la institución bancaria y utilizarlo inadvertidamente para fines fraudulentos.

Lo anterior se concluye y demuestra de las debilidades de seguridad del Sistema de Software "AS" antes mencionado. Estas debilidades y su explotación por parte de un atacante con conocimientos básicos de, software, redes y sistemas computacionales, se detallan y describen en las respuestas a las Preguntas I, II y III de este mismo dictamen así como también en las Secciones 1.1, 1.2, 1.3 y 1.4 del Anexo Técnico de este mismo dictamen.

Un resumen de estas debilidades y su explotación maliciosa por parte de un atacante con conocimientos básicos de, software, redes y sistemas computacionales, es el siguiente:

1) El sistema de software AS no implementa el concepto de firma digital ni de autenticadores biométricos para autenticar e identificar a los cajeros y a los funcionarios, tales como subgerentes. Tanto cajeros como

subgerentes utilizan, en el sistema AS, claves y contraseñas débiles para realizar y autorizar operaciones bancarias. Las implicaciones de seguridad que tiene un sistema de software que no implementa firma digital ni autenticadores biométricos, se describen con detalle en la Sección 1.1 del Anexo Técnico de este mismo dictamen.

2) Un atacante con conocimientos básicos de, software, redes y sistemas computacionales, puede fácilmente apoderarse de las claves y contraseñas de manera inadvertida y realizar con ellas las mismas operaciones que el cajero y subgerente legítimos. La forma en que un atacante se puede apoderar de claves y contraseñas se describen con detalle en las Secciones 1.2 del Anexo Técnico de este mismo dictamen.

3) Cualquier atacante con conocimientos básicos de, software, redes y sistemas computacionales, puede fácilmente vulnerar los controles de seguridad del Sistema de Software antes mencionado y de las propias instalaciones de la institución bancaria y de su sucursal, ya que no cumplían, a la fecha de los hechos, con las recomendaciones de seguridad que exigen los estándares nacionales e internacionales, tales como el ISO 17799 y el ISO 27001. Lo anterior se describe con detalle en la Respuesta a la Pregunta III de este mismo dictamen.

5) Dictaminar si personas no autorizadas pueden acceder a las instalaciones de la institución bancaria –matriz- y de su sucursal, lugar físico desde el cual se operó el mencionado sistema de software.

Respuesta:

Cualquier persona (todos los cajeros, todos los funcionarios encargados de autorizar operaciones como son los subgerentes, personal de mantenimiento de los equipos de cómputo y otros funcionarios del propio banco) con acceso físico al área de cajas podía tener acceso a los equipos de cómputo, tanto a los equipos de cómputo donde se ejecuta el proceso cliente de la aplicación AS como al equipo de cómputo donde se ejecuta el proceso servidor de la misma aplicación AS. Lo anterior lo pudo constatar el perito en la diligencia presencial que realizó el día 23 de Junio de 2010 a las instalaciones de la institución bancaria en su sucursal, desde donde presuntamente se realizaron los movimientos irregulares. En el dictamen original se anexo un diagrama que muestra la ubicación física del área mencionada donde se señala la ubicación de los equipos de cómputo donde se ejecuta el proceso cliente de la aplicación AS y la ubicación del equipo de cómputo donde se ejecuta el proceso servidor de aplicación AS. Este esquema no se podrá mostrar para no violar el convenio de confidencialidad.

Cualquiera de todas las personas mencionadas pudo haber explotado cualquiera o todas las debilidades del sistema de software AS, descritas con detalle en las respuestas a las Preguntas I, II y III de este mismo dictamen así como también en las Secciones 1.1, 1.2, 1.3 y 1.4 del Anexo Técnico de este mismo dictamen, para apoderarse de claves y contraseñas de acceso no sólo a la aplicación cliente sino también a la aplicación servidor y, con ello, realizar prácticamente todas las operaciones que deseara, de manera ilícita.

6) Dictaminar si, con los argumentos y evidencias informáticas expuestas por la institución bancaria y sus peritos, es posible que los C.cajera1 y subgerente hayan podido realizar en lugar, tiempo y forma, las transferencias fraudulentas de las cuales se les acusa.

Respuesta:

Con los argumentos y evidencias informáticas expuestas por la institución bancaria y sus peritos, NO es posible que los C. cajera1 y subgerente hayan podido realizar en lugar, tiempo y forma, las operaciones presuntamente fraudulentas de las cuales se les acusa.

El dictamen de este punto se basa en lo que a continuación se argumenta:

1) El total de operaciones de depósito, supuestamente fraudulentas, fue de 45 (cuarenta y cinco) realizadas, de manera consecutiva, en un lapso de tiempo de 1:08:56 (1 hora, 08 minutos, 56 segundos).

2) El total de tiempo de las operaciones que duraron alrededor de 1 minuto y el número de operaciones realizadas arroja un promedio de 52 segundos por operación, 40 (cuarenta) de las cuales requirieron de la autorización del subgerente para ser realizadas.

3) El tiempo mínimo en la realización de una operación, que requirió la autorización del subgerente, de acuerdo a la vista mostrada en la Figura No. 2 de este dictamen, fue de 00:00:46 (cuarenta y seis segundos)

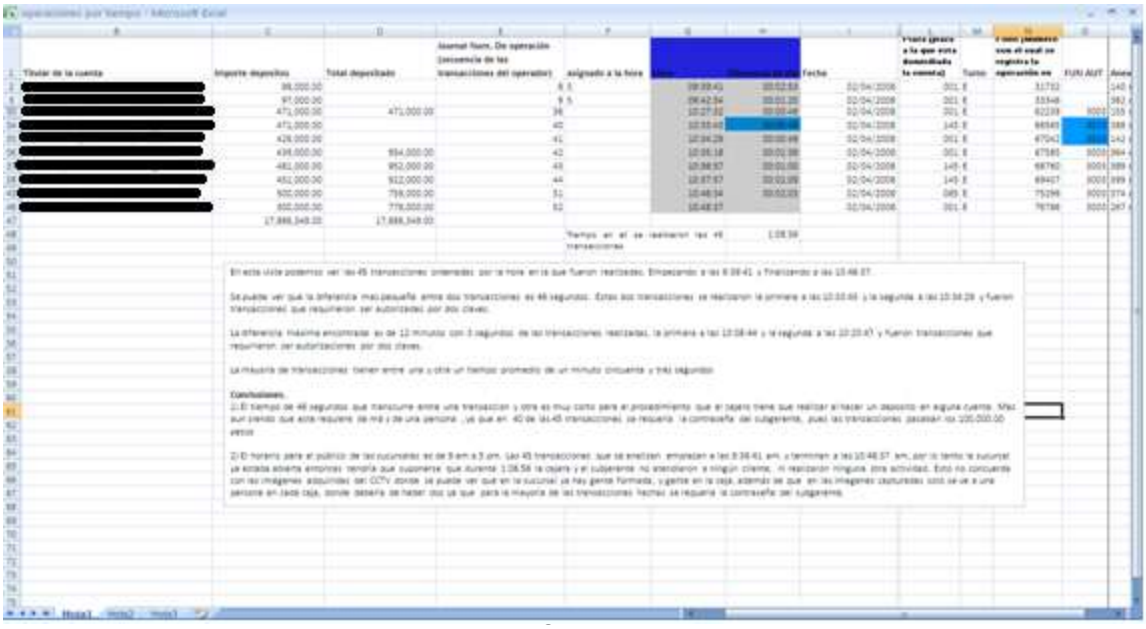


Figura 5.22. Operaciones por Tiempo.

4) Tomando en cuenta la recreación y la operación del sistema de software AS, presenciada por el perito, estos tiempos no pueden ser humanamente posibles, dado que los depósitos fueron hechos a diferentes números de cuenta, plazas y nombres de clientes distintos, datos que tuvieron que ser leídos de un papel o dictados por una persona.

5) También significaría, en el caso de que los inculpados las hubieran realizado, que, durante el lapso de tiempo de 1:08:56 (1 hora, 08 minutos, 56 segundos), tanto la cajera 1 como el subgerente, no realizaron otro tipo de operaciones ni atendieron a ninguna persona en ese periodo de tiempo, lo que contradice las imágenes de Circuito Cerrado de TV (CCTV) proporcionadas por la institución bancaria en donde se observa una fila de personas siendo atendidas por los cajeros.

6) El estudio y análisis de las imágenes de Circuito Cerrado de TV (CCTV) proporcionadas por la institución bancaria al perito, que obran en el expediente de la causa, con las cuales la institución bancaria pretende demostrar que los inculpados, cajera 1 y subgerente, se encontraban en tiempo, forma y lugar para realizar las operaciones presuntamente fraudulentas de las cuales se les acusa, permite al perito obtener las siguientes conclusiones:

    a. Las imágenes de referencia fueron editadas, es decir, alteradas, ya que fueron entregadas al perito en un formato ppt (Power Point), el cual no corresponde al formato original del dispositivo que graba y almacena esas imágenes. Cualquier persona con conocimientos básicos de cómputo puede notar esta alteración ya que, por ejemplo el encabezado de las imágenes

(**D:\01_aSuNtOs aFjR\Asunto_SucursalBancaria\Nombre de la Sucursal**) de ninguna manera corresponde al formato original que entrega el dispositivo.

b. Aun cuando las imágenes no hubieran sido alteradas, en las imágenes se aprecia claramente que, en la Caja No. 1 quien aparece en ese momento es un hombre y no una mujer como sería de esperarse si se tratara de la cajera principal inculpada Cajera 1. También se aprecia en la segunda imagen que la persona de sexo masculino frente a la caja no está operando el teclado de la computadora, actividad indispensable en el caso de haber estado relacionado con las operaciones de depósito supuestamente fraudulentas.

c. Las imágenes de Circuito Cerrado de TV (CCTV), proporcionadas por la institución bancaria al perito, demuestran justamente lo contrario de lo que la institución bancaria pretende demostrar. Demuestran claramente que la inculpada del sexo femenino NO SE ENCONTRABA físicamente en ese momento en ese lugar desde el cual supuestamente se realizaron las operaciones de depósito supuestamente fraudulentas.

d. La hora que muestran las imágenes de Circuito Cerrado de TV (CCTV) proporcionadas por la institución bancaria al perito no se encuentran dentro del lapso de tiempo en que se realizaron las operaciones supuestamente fraudulentas, las cuales fueron realizadas entre las 09:39:41 (9 horas, 39 minutos, 41 segundos) y las 10:48:37 (10 horas, 48 minutos, 37 segundos). Esto demuestra que NO EXISTE evidencia NI PRUEBA temporal alguna que demuestre que los inculpados se encontraban en el lapso de tiempo y en el lugar durante el cual y en el cual se

realizaron las operaciones de depósito supuestamente fraudulentas.

e. Al realizar el análisis de los metadatos de las imágenes proporcionadas por la institución bancaria al perito informático, se encontró que estas habían sido modificadas durante un tiempo de 00:5:54 (5 minutos, 54 segundos). Al no conservarse la integridad de la evidencia, esta no puede tomarse en cuenta como válida.

7) Dictamine si existen fundamentos técnicos y teóricos para relacionar, de manera incontrovertible, una contraseña, clave o password con la persona que la utiliza.

Respuesta:

NO existen fundamentos técnicos para relacionar, de manera incontrovertible, una contraseña, clave o clave con la persona que la utiliza.

No existe fundamento, ni técnico, ni científico, ni teórico, ni práctico, para relacionar la identidad de una persona con una contraseña o clave. El poseer una contraseña o clave nada tiene que ver con la identidad real de quien la posee. El que la posee o conoce, en un momento dado, puede ser una persona o proceso totalmente distinto de la persona o proceso que autorizadamente debiera poseerla y conocerla.

Lo anterior se debe a que una contraseña o clave no es un elemento inherente a la naturaleza física y biológica del que la posee como, por ejemplo, sí lo son el DNA o la huella dactilar.

Una contraseña puede ser robada, puede ser adivinada, puede ser expresamente rota con programas de cómputo, puede ser conocida por los

administradores de un sistema como el denominado “AS” de la institución bancaria, puede ser conocida durante su viaje por el canal de red con programas de cómputo

Una vez que una entidad, persona o proceso logra conocer la clave o contraseña de otra persona, entidad o proceso puede hacer con esa clave o contraseña lo mismo que hace la legítima poseedora de la misma. Por ejemplo, entre otras cosas, puede realizar operaciones y transferencias como si fuera la legítima poseedora.

Un sistema de software que basa la identificación de una persona en una contraseña o clave no puede, ni debe, pretender demostrar la realización de un hecho con esa persona, argumentando que ese hecho se realizó con la contraseña que esa persona conocía. Eso no tiene sentido, ni justificación técnica ni científica.

Lo más parecido, en sistemas de identificación y autenticación, a la identificación real biológica es la utilización de autenticadores biométricos o de lo que se conoce como firma digital. Ninguno de estos conceptos y autenticadores están implementados en el sistema denominado “AS” de la institución bancaria.

Información detallada sobre estos conceptos se describen en la Sección 1.1 del Anexo Técnico correspondiente a este dictamen.

8) **Dictaminar si la institución bancaria cumplía, a la fecha de los hechos, con las auditorías que la Comisión Nacional Bancaria y de Valores realiza anualmente a las instituciones de su tipo y con las recomendaciones que dicha comisión emite. En particular si cumplía, a la fecha de los hechos, con las auditorías y sus recomendaciones al sistema AS.**

Respuesta:

La institución bancaria NO cumplía, a la fecha de los hechos, con las auditorías que la Comisión Nacional Bancaria y de Valores realiza anualmente a las instituciones de su tipo y con las recomendaciones que dicha comisión emite. En particular si cumplía, a la fecha de los hechos, con las auditorías y sus recomendaciones al sistema AS.

La institución bancaria a la petición explícita del perito de proporcionar: "*Copias certificadas de los resultados de las Auditorías de de la Comisión Nacional Bancaria y de Valores realizadas a la institución bancaria sobre el sistema AS y sistemas relacionados durante el año 2008 y, en su caso, del año 2007*" respondió lo siguiente: "*En las visitas realizadas por la Comisión Nacional Bancaria y de Valores durante los años 2007 y 2008, dicha autoridad no realizó auditorias al sistema AS ni a sistemas relacionados*"

Lo anterior quiere decir que sí hubo visitas por parte de la Comisión Nacional Bancaria y de Valores a la institución bancaria pero, según la citada institución bancaria, no se realizó auditoría alguna al sistema AS ni a sistemas relacionados. Pero no se muestra evidencia de que realmente fue así.

Lo anterior lleva al perito a concluir que la institución bancaria NO cumplía, a la fecha de los hechos, con las recomendaciones que dicha comisión emite y que el sistema AS no había sido auditado, por parte de la Comisión Nacional de Banca y de Valores, durante los años 2007 y 2008.

Tales recomendaciones de la Comisión Nacional Bancaria y de Valores se expresan en la LEY DE LA COMISION NACIONAL BANCARIA Y DE VALORES, publicada en el Diario Oficial de la Federación el 28 de abril de 1995. Actualizada con las modificaciones del Decreto por el que se expide la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo y se reforman, adicionan y derogan diversas disposiciones de la Ley General de Sociedades

Cooperativas, de la Ley de Ahorro y Crédito Popular, de la Ley de la Comisión Nacional Bancaria y de Valores y de la Ley de Instituciones de Crédito, publicado en el Diario Oficial de la Federación el 13 de agosto de 2009.

9) **Dictaminar si, conociendo las claves necesarias, es indispensable el ingresar al sistema desde los equipos involucrados, o, en su caso si el sistema AS permitía, a la fecha de los hechos, que cualquier persona ingresara con la calidad de cajero o subgerente al mismo desde cualquier equipo de la sucursal en cuestión u otra. En su caso indique si el personal de informática de la Institución bancaria podría ingresar, a la fecha de los eventos desde sus propias terminales utilizando las claves de cajeros, subgerentes o gerentes.**

Respuestas:

Conociendo las claves necesarias, NO es indispensable el ingresar al sistema desde los equipos de cómputo involucrados.

El sistema de software AS de la institución bancaria es un sistema cliente/servidor que opera en red y que no valida el hardware desde el cual se puede ejecutar la aplicación cliente. Este hecho permite que cualquier persona o proceso que conozca las claves o contraseñas correspondientes pueda ingresar al sistema y suplantar al legítimo proceso cliente, pudiendo realizar en su nombre operaciones fraudulentas.

Lo anterior también es posible realizarlo desde aplicaciones de software específicamente diseñadas para ello, tal como la aplicación **NetView Dm/2*** que

se encontró instalada en los equipos involucrados, específicamente en el equipo en el que se ejecutaba el proceso servidor de la aplicación AS.

El sistema AS, SÍ permitía, a la fecha de los hechos, que cualquier persona, que supiera las claves o contraseñas, ingresará con la calidad de cajero o subgerente al mismo desde cualquier equipo de la sucursal en cuestión u otra.

El personal de informática de la Institución SÍ podía ingresar al sistema AS, a la fecha de los eventos, desde sus propias terminales utilizando las claves de cajeros, subgerentes o gerentes.

10) Dictaminar si los argumentos y evidencias informáticas, fotográficas y de videograbación expuestas por la institución bancaria y sus peritos coinciden en lugar, tiempo, forma y circunstancia con las ubicaciones, tiempos, formas y circunstancias de los inculpados, en el intervalo de tiempo durante el cual se realizaron las operaciones presuntamente fraudulentas y permiten concluir que los hoy inculpados realizaron efectivamente las operaciones cuestionadas, y, en su caso indique si las declaraciones de los peritos presentados por la institución bancaria están debidamente fundadas en los hechos y las técnicas periciales internacionalmente aceptadas.

Respuesta:

Los argumentos y evidencias informáticas, fotográficas y de videograbación expuestas por la institución bancaria y sus peritos NO coinciden en lugar, tiempo, forma y circunstancia con las ubicaciones, tiempos, formas y circunstancias de los inculpados, en el intervalo de tiempo durante el cual se realizaron las operaciones presuntamente fraudulentas.

Los argumentos y evidencias informáticas, fotográficas y de videograbación expuestas por la institución bancaria y sus peritos NO permiten concluir que los hoy inculpados realizaron efectivamente las operaciones cuestionadas.

Con los argumentos y evidencias informáticas expuestas por la institución bancaria y sus peritos, NO es posible que los C. Cajera 1 y Subgerente hayan podido realizar en lugar, tiempo y forma, las operaciones presuntamente fraudulentas de las cuales se les acusa.

El dictamen de este punto se basa en lo que a continuación se argumenta:

1) El total de operaciones de depósito, supuestamente fraudulentas, fue de 45 (cuarenta y cinco) realizadas, de manera consecutiva, en un lapso de tiempo de 1:08:56 (1 hora, 08 minutos, 56 segundos).

2) El total de tiempo de las operaciones realizadas en alrededor de 1 minuto y el número de operaciones realizadas arroja un promedio de 52 segundos por operación, 40 (cuarenta) de las cuales requirieron de la autorización del subgerente para ser realizadas.

3) El tiempo mínimo en la realización de una operación, que requirió la autorización del subgerente, de acuerdo a la vista mostrada en la Figura No. 2 de este dictamen, fue de 00:00:46 (cuarenta y seis segundos)

4) Tomando en cuenta la recreación y la operación del sistema de software AS, presenciada por el perito, estos tiempos no pueden ser humanamente posibles, dado que los depósitos fueron hechos a diferentes números de cuenta, plazas y nombres de clientes distintos, datos que tuvieron que ser leídos de un papel o dictados por una persona.

5) También significaría, en el caso de que los inculpados las hubieran realizado, que, durante el lapso de tiempo de 1:08:56 (1 hora, 08 minutos, 56 segundos), tanto la Cajera 1 como el Subgerente, no realizaron otro tipo de operaciones ni atendieron a ninguna persona en ese periodo de tiempo, lo que contradice las imágenes de Circuito Cerrado de TV (CCTV) proporcionadas por la institución bancaria al perito donde se observa una fila de personas siendo atendidas por los cajeros.

6) El análisis estadístico de todas las operaciones supuestamente fraudulentas realizadas, se muestra en las Figuras 5.22, 5.23, 5.24 y 5.25.

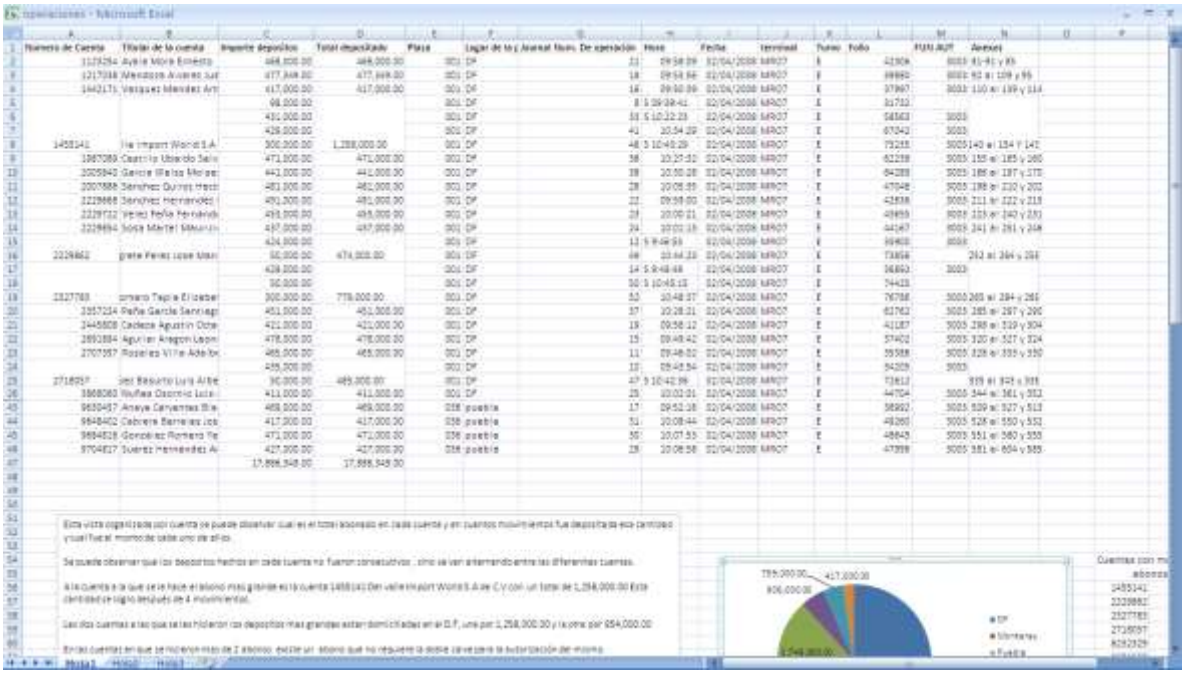


Figura 5.23 Operaciones.

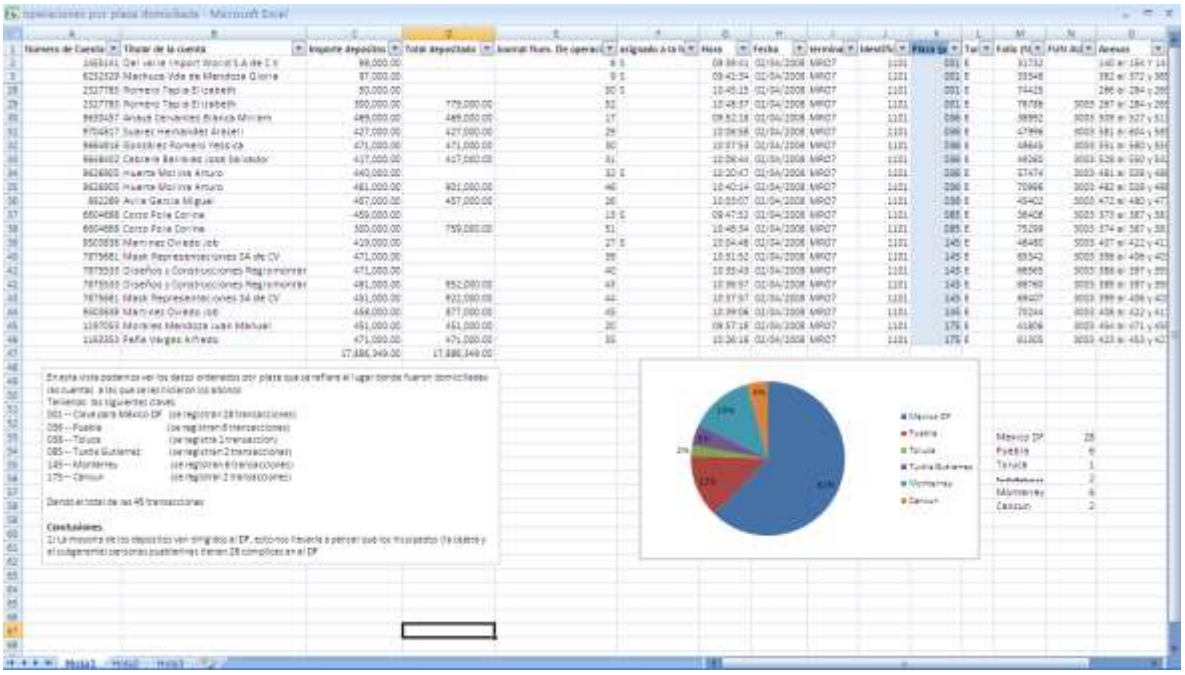


Figura 5.24 Operaciones por plaza domiciliada.

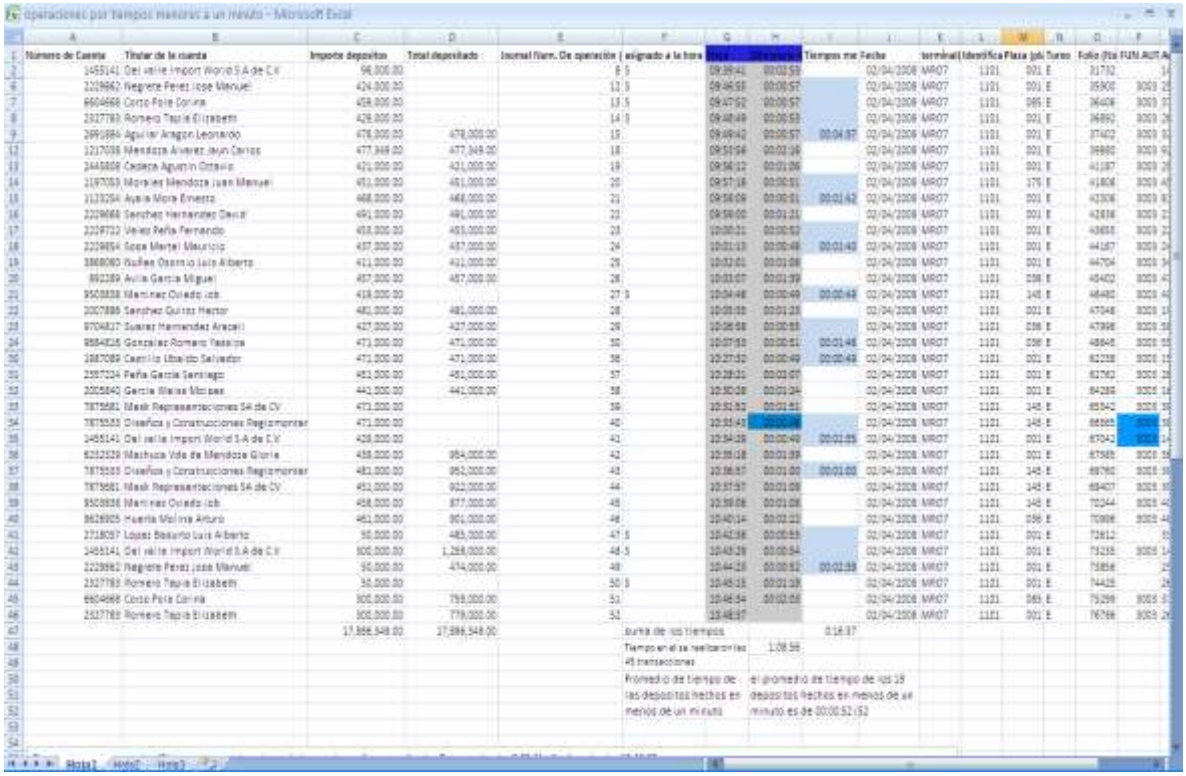


Figura 5.25 Operaciones por tiempo menor a un minuto.

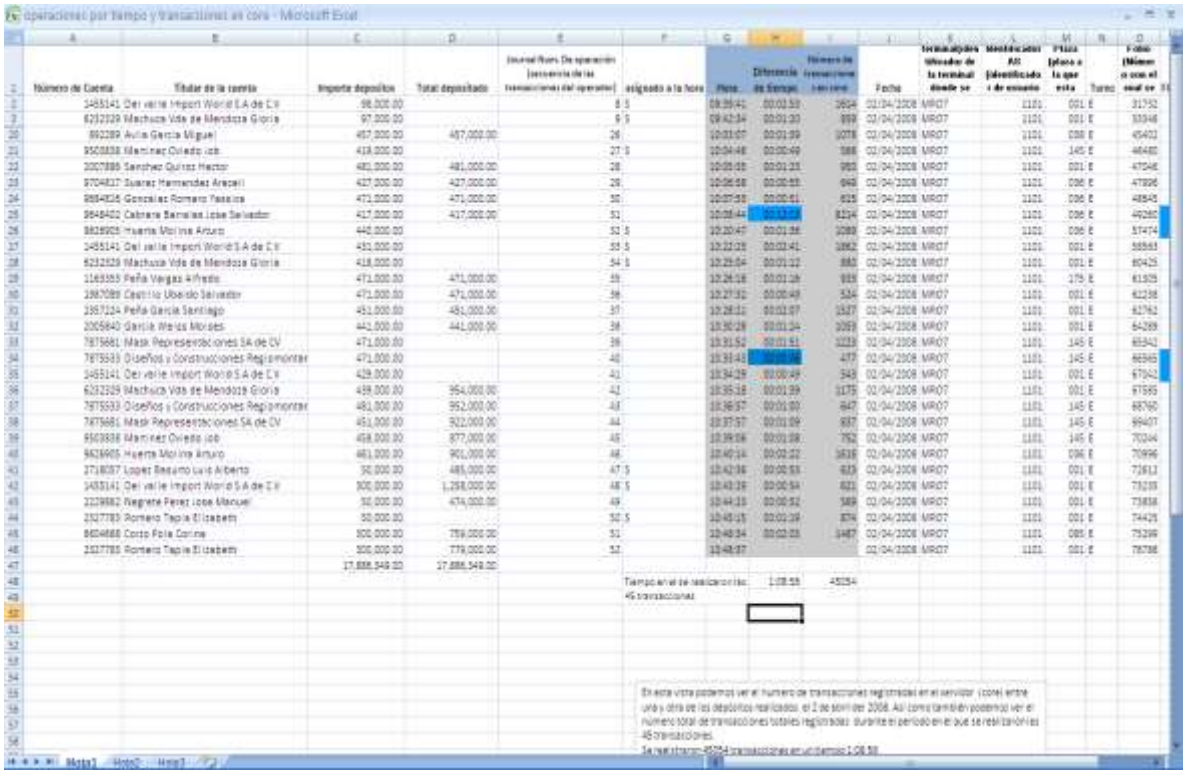


Figura 5.26 Operaciones por tiempo y transacción en el core.

El estudio y análisis de las imágenes de Circuito Cerrado de TV (CCTV) proporcionadas por la institución bancaria al perito, que obran en el expediente de la causa, con las cuales la institución bancaria pretende demostrar que los inculpados, Cajera 1 y Subgerente, se encontraban en tiempo, forma y lugar para realizar las operaciones presuntamente fraudulentas de las cuales se les acusa, permite al perito obtener las siguientes conclusiones:

a. Las imágenes de referencia fueron editadas, es decir, alteradas, ya que fueron entregadas al perito en un formato ppt (Power Point), el cual no corresponde al formato original del dispositivo que graba y almacena esas imágenes. Cualquier persona con conocimientos básicos de cómputo puede notar esta alteración ya que, por ejemplo el encabezado de las imágenes (**D:\01_aSuNtOs aFjR\Asunto_SucursalBancaria\Nombre de la**

Sucursal)de ninguna manera corresponde al formato original que entrega el dispositivo.

b. Aún cuando las imágenes no hubieran sido alteradas, en las imágenes se aprecia claramente que, en la Caja No. 1, quien aparece en ese momento es un hombre y no una mujer como sería de esperarse si se tratara de la cajera principal inculpada Cajera 1. También se aprecia en la segunda imagen que la persona de sexo masculino frente a la caja no está operando el teclado de la computadora, actividad indispensable en el caso de haber estado relacionado con las operaciones de depósito supuestamente fraudulentas.

c. Las imágenes de Circuito Cerrado de TV (CCTV), proporcionadas por la institución bancaria al perito, demuestran justamente lo contrario de lo que la institución bancaria pretende demostrar. Demuestran claramente que la inculpada del sexo femenino NO SE ENCONTRABA físicamente en ese momento en ese lugar desde el cual supuestamente se realizaron las operaciones de depósito supuestamente fraudulentas.

La hora de las imágenes de Circuito Cerrado de TV (CCTV) proporcionadas por la institución bancaria al perito no se encuentran dentro del lapso de tiempo en que se realizaron las operaciones supuestamente fraudulentas, las cuales fueron realizadas entre las 09:39:41 (9 horas, 39 minutos, 41 segundos) y las 10:48:37 (10 horas, 48 minutos, 37 segundos). Esto demuestra que NO EXISTE evidencia NI PRUEBA temporal alguna que demuestre que los inculpados se encontraban en el lapso de tiempo y en el lugar durante el cual y en el cual se realizaron las operaciones de depósito supuestamente fraudulentas.

Las declaraciones de los peritos presentados por la institución bancaria NO están debidamente fundadas en los hechos y las técnicas periciales internacionalmente aceptadas.

Respecto a este último párrafo, el dictamen se basa en lo siguiente:

1) La cadena de custodia de las evidencias, tales como equipos de cómputo, bitácoras, grabaciones del circuito cerrado de TV, entre otras, del caso, no fue cumplida ni respetada por la institución bancaria y sus peritos.

2) La evidencia de lo anterior se documenta con las metodologías internacionalmente aceptadas en la materia.

3) La institución bancaria no pudo demostrar ni dar ninguna garantía, de ningún tipo, al perito de que las evidencias no hubieran sido modificadas, alteradas o eliminadas por la institución bancaria.

4) El resguardo y vigilancia de las evidencias nunca estuvo en poder de la autoridad competente en ningún momento como indican los estándares nacionales e internacionales en la materia.

5) El resguardo y vigilancia de las evidencias siempre estuvo a cargo de la institución bancaria, lo que le quita toda validez a sus argumentos basados en esas evidencias, ya que la institución bancaria pudo haber alterado, borrado o modificado tales evidencias de acuerdo a sus intereses y conveniencias.

11) Dictaminar si existe evidencia para demostrar que las operaciones fraudulentas imputables a los acusados fueron en realidad realizadas por un proceso o programa de software, sembrado en los equipos y programas de la institución bancaria por terceras personas, y no por los inculpados.

Respuesta:

A partir del análisis forense que el perito realizó sobre la información contenida en los discos duros de los equipos de cómputo que ejecutan tanto el proceso cliente como el proceso servidor, de la aplicación de software cliente/servidor AS de la institución bancaria, se encontró, respecto a este punto del dictamen, lo siguiente:

1) En el disco duro del equipo de cómputo donde se ejecuta el proceso servidor, de la aplicación de software cliente/servidor AS, se encontró instalado la aplicación de software de nombre **NetView Dm/2***, la cual, de manera general, se puede decir que permite la comunicación de un servidor con otro, así como también permite la administración de software o aplicaciones de manera remota.

2) Por medio de la aplicación **NetView Dm/2***, se pueden ejecutar las sesiones cliente (aplicaciones que usan los cajeros para realizar operaciones bancarias) que se deseen y realizar con ellas las mismas operaciones que realiza un cajero frente a ventanilla.

3) Por medio de la aplicación **NetView Dm/2***, las sesiones cliente y las operaciones bancarias mencionadas en el punto 3 anterior, se pueden realizar de manera remota por una persona distinta al cajero.

4) Lo descrito en los puntos 1, 2 y 3 anteriores abre totalmente la posibilidad de que las operaciones fraudulentas imputadas a los inculpados hayan sido realizadas en realidad por medio de este software, desde la computadora que ejecuta el proceso servidor de la aplicación AS y por terceras personas distintas a los inculpados.

5) Al analizar los registros de bitácora (archivo MESSAGE.DAT) de la aplicación **NetView Dm/2***, llama la atención lo siguiente:

   - ✓ Únicamente existe un registro del día del incidente, es decir, 02/04/2008 (2 de Abril del 2008).

   - ✓ Después de los registros con fecha del 03/04/2008 (3 de Abril del 2008) los registros comienzan a aparecer con fecha de 01/01/1980 (1 de Enero de 1980), para reaparecer de nuevo con fecha del 4 y 5 de Abril de 2008.

   - ✓ Al parecer la secuencia de aparición en orden cronológico de los registros fue alterada o cambiada o bien pudieron haber sido borrados algunos registros justo en los rangos de fechas de ocurrencia del incidente.

6) Este comportamiento anómalo hace pensar que dichos registros pudieron ser modificados al saber que dichos registros contienen información de conexiones con el servidor, o tienen la capacidad de mostrar si se instaló alguna aplicación o software de forma remota, o si se instaló algún software malicioso, o si hubiese existido alguna conexión indebida al servidor.

12) Dictaminar si se ha modificado en algún momento el medio de identificación electrónica otorgado a los inculpados, en caso afirmativo indicar en qué fecha, desde que equipos fue realizado esa modificación, quienes pueden realizarla y que claves se requieren para ello.

Respuesta:

Entendido el medio de identificación electrónica como la clave o contraseña que los inculpados utilizan para identificarse mediante el proceso cliente ante el proceso servidor de la aplicación de software AS de la institución bancaria, la referida institución bancaria, a pregunta expresa del perito a este respecto, respondió textualmente lo siguiente:

> "*Las contraseñas son de carácter alfanumérico. Asimismo, requieren al usuario el cambio periódico obligatorio, cuentan con longitudes mínimas máximas y se validan los caracteres repetidos. Por otro lado, las contraseñas tienen un periodo de caducidad y se obliga al usuario su cambio cuando se utiliza por primera vez*"

No obstante, la institución bancaria, no mostró evidencia de tener implementado en el sistema de software AS ningún control de seguridad respecto a esta política, ni se encontró evidencia alguna en bitácoras de que se hubiera ejecutado o realizado cambio alguno en dicho medio de identificación de los inculpados.

13) Dictaminar si pudo un tercero por medios presenciales o remotos operar los equipos involucrados en el fraude habiendo capturado las claves necesarias.

Respuesta:

En efecto, un tercero SÍ pudo, por medios presenciales o remotos, operar los equipos involucrados en el fraude habiendo capturado las claves necesarias.

Conociendo las claves necesarias, NO es indispensable el ingresar al sistema desde los equipos de cómputo involucrados.

El sistema de software AS de la institución bancaria es un sistema cliente/servidor que opera en red y que no valida el hardware desde el cual se puede ejecutar la aplicación cliente. Este hecho permite que cualquier persona o proceso que conozca las claves o contraseñas correspondientes pueda ingresar al sistema y suplantar al legítimo proceso cliente pudiendo realizar en su nombre operaciones fraudulentas.

Lo anterior también es posible realizarlo desde aplicaciones de software específicamente diseñadas para ello, tal como la aplicación **NetView Dm/2*** que se encontró instalada en los equipos involucrados, específicamente en el equipo en el que se ejecutaba el proceso servidor de la aplicación AS.

El sistema AS, SÍ permitía, a la fecha de los hechos, que cualquier persona, que supiera las claves o contraseñas, ingresara con la calidad de cajero o subgerente al mismo desde cualquier equipo de la sucursal en cuestión u otra.

El sistema de software AS de la institución bancaria es un sistema cliente/servidor que opera en red y que no valida el hardware desde el cual se puede ejecutar la aplicación cliente. Este hecho permite que cualquier persona o proceso que conozca las claves o contraseñas correspondientes puede ingresar al sistema y suplantar al legítimo proceso cliente pudiendo realizar en su nombre operaciones fraudulentas.

Lo anterior también es posible realizarlo desde aplicaciones de software específicamente diseñadas para ello, tal como la aplicación **NetView Dm/2*** que se encontró instalada en los equipos involucrados, específicamente en el equipo en el que se ejecutaba el proceso servidor de la aplicación AS

El personal de informática de la Institución SÍ podía ingresar al sistema AS, a la fecha de los eventos, desde sus propias terminales utilizando las claves de cajeros, subgerentes o gerentes.

14) Dictaminar si se pueden realizar operaciones remotas desde los equipos involucrados, y en su caso, expresar que mecanismos pueden utilizarse para ello y si existe instalado en los equipos involucrados o cualquier otro de la sucursal el software necesario a esos efectos.

Respuesta:

SÍ se pueden realizar operaciones remotas desde los equipos involucrados.

Se pudieron haber realizado utilizando mecanismos de software como el que se encontró, mediante análisis forense, instalado en el disco duro del equipo de cómputo donde se ejecuta el proceso servidor, de la aplicación de software cliente/servidor AS. Se encontró instalada la aplicación de software de nombre **NetView Dm/2**, la cual, de manera general, se puede decir que permite la comunicación de un servidor con otro, así como también permite la administración de software o aplicaciones de manera remota.

Por medio de la aplicación **NetView Dm/2**, se pueden ejecutar las sesiones cliente (aplicaciones que usan los cajeros para realizar operaciones bancarias) que se deseen y realizar con ellas las mismas operaciones que realiza un cajero frente a ventanilla.

Por medio de la aplicación **NetView Dm/2**, las sesiones cliente y las operaciones bancarias mencionadas en el punto 3 anterior, se pueden realizar de manera remota por una persona distinta al cajero.

Lo descrito anteriormente abre totalmente la posibilidad de que las operaciones fraudulentas imputadas a los inculpados hayan sido realizadas en realidad por medio de este software, desde la computadora que ejecuta el proceso servidor de la aplicación AS y por terceras personas distintas a los inculpados.

Conociendo las claves necesarias, NO es indispensable el ingresar al sistema desde los equipos de cómputo involucrados.

El sistema de software AS de la institución bancaria es un sistema cliente/servidor que opera en red y que no valida el hardware desde el cual se puede ejecutar la aplicación cliente. Este hecho permite que cualquier persona o proceso que conozca las claves o contraseñas correspondientes puede ingresar al sistema y suplantar al legítimo proceso cliente pudiendo realizar en su nombre operaciones fraudulentas.

Lo anterior también es posible realizarlo desde aplicaciones de software específicamente diseñadas para ello, tal como la aplicación **NetView Dm/2** que se encontró instalada en los equipos involucrados, específicamente en el equipo en el que se ejecutaba el proceso servidor de la aplicación AS.

El sistema AS, SÍ permitía, a la fecha de los hechos, que cualquier persona, que supiera las claves o contraseñas, ingresara con la calidad de cajero o subgerente al mismo desde cualquier equipo de la sucursal en cuestión u otra.

El sistema de software AS de la institución bancaria es un sistema cliente/servidor que opera en red y que no valida el hardware desde el cual se puede ejecutar la aplicación cliente. Este hecho permite que cualquier persona o proceso que conozca las claves o contraseñas correspondientes pueda ingresar al sistema y suplantar al legítimo proceso cliente pudiendo realizar en su nombre operaciones fraudulentas.

Lo anterior también es posible realizarlo desde aplicaciones de software específicamente diseñadas para ello, tal como la aplicación **NetView Dm/2** que se encontró instalada en los equipos involucrados, específicamente en el equipo en el que se ejecutaba el proceso servidor de la aplicación AS

El personal de informática de la institución bancaria SÍ podía ingresar al sistema AS, a la fecha de los eventos, desde sus propias terminales utilizando las claves de cajeros, subgerentes o gerentes.

15) Dictaminar si hubo la posibilidad de operar los equipos en forma remota, bajo las condiciones de seguridad informática vigentes a la fecha del suceso.

Respuesta:

SÍ es posible operar los equipos, y las aplicaciones instaladas en ellos, en forma remota, bajo las condiciones de seguridad informática vigentes a la fecha del suceso.

En el disco duro del equipo de cómputo donde se ejecuta el proceso servidor, de la aplicación de software cliente/servidor AS, se encontró, mediante el análisis forense, instalado la aplicación de software de nombre **NetView Dm/2**, la cual, de manera general, se puede decir que permite la comunicación de un

servidor con otro, así como también permite la administración de software o aplicaciones de manera remota.

Por medio de la aplicación **NetView Dm/2**, se pueden ejecutar las sesiones cliente (aplicaciones que usan los cajeros para realizar operaciones bancarias) que se deseen y realizar con ellas las mismas operaciones que realiza un cajero frente a ventanilla.

Por medio de la aplicación **NetView Dm/2**, las sesiones cliente y las operaciones bancarias mencionadas en el punto 3 anterior, se pueden realizar de manera remota por una persona distinta al cajero.

Lo descrito anteriormente abre totalmente la posibilidad de que las operaciones fraudulentas imputadas a los inculpados hayan sido realizadas en realidad por medio de este software, desde la computadora que ejecuta el proceso servidor de la aplicación AS y por terceras personas distintas a los inculpados.

16) Dictaminar, por medio del análisis forense de los registros de la Institución Bancaria las bitácoras de operación completas de las reparaciones realizadas al cajero automático de la sucursal para demostrar las actividades de los sujetos a proceso.

Respuesta:

No se tuvo acceso a los equipos de cómputo involucrados con la operación y reparaciones realizadas al cajero automático.

La institución bancaria no proporcionó las grabaciones de video del sistema de Circuito Cerrado de TV (CCTV) a pesar de que se le solicitó oficialmente.

La institución bancaria sólo proporcionó, a este respecto, dos imágenes editadas y en un formato que no corresponden al formato original del modelo March 41165, modelo que corresponde al que la institución bancaria posee y estaba en operación al momento del incidente.

Este modelo posee un monitor con un temporizador para ver todas las cámaras y que realiza capturas de una imagen por segundo y que graba las imágenes de forma continua en los discos duros.

Es importante resaltar que el modelo del sistema de vigilancia que se nos indicó esta descontinuado, o no existe ya en el mercado. Esto se constata en la página web oficial de la marca correspondiente, en la cual aparecen solo modelos similares y de la misma serie.

En cuanto al software utilizado por este dispositivo de grabación de imágenes de CCTV, la página oficial de la marca menciona que todos sus dispositivos utilizan el software **VideoSphere**, el cual realiza las grabaciones con un formato **mpg** y se pueden obtener en formato **jpg** si se cuenta con el software adicional, ninguno de estos dos formatos corresponde al formato entregado por la institución bancaria.

Las imágenes entregadas por la institución bancaria fueron en formato .ppt, el cual corresponde al software de Microsoft Office conocido como Power Point.

La página oficial de la marca MARCH es: http://www.marchnetworks.com/

17) Dictaminar y explicar cuál es el procedimiento necesario para llevar a cabo las reparaciones del cajero automático y si se requiere la presencia de alguna persona a esos efectos, en su caso, cuáles serían esas personas y si existen claves o identificadores para esa operación.

Respuesta:

No se tuvo acceso a ninguna información, procedimientos, bitácoras o equipos relacionados con este punto del dictamen.

18) Dictaminar, de acuerdo al punto anterior sobre la presencia de alguno o ambos inculpados en el cajero automático al momento en que ocurren las operaciones bajo análisis.

Respuesta:

La institución bancaria no proporcionó las grabaciones de video del sistema de Circuito Cerrado de TV (CCTV) a pesar de que se le solicitó oficialmente.

La institución bancaria sólo proporcionó, a este respecto, dos imágenes editadas y en un formato que no corresponden al formato original del modelo March 41165, modelo que corresponde al que la institución bancaria posee y estaba en operación al momento de ocurrir el incidente.

Las imágenes proporcionadas por institución bancaria no cubren el área de cajeros automáticos, por lo que no se puede asegurar ni negar nada respecto a que si los involucrados estuvieron o no en el área del cajero automático en el lapso de tiempo durante el cual ocurrieron las operaciones bajo análisis.

Este modelo posee un monitor con un temporizador para ver todas las cámaras y que realiza capturas de una imagen por segundo y que graba las imágenes de forma continua en los discos duros.

Es importante resaltar que el modelo del sistema de vigilancia que se nos indicó esta descontinuado, o no existe ya en el mercado. Esto se constata en la página web oficial de la marca correspondiente, en la cual aparecen solo modelos similares y de la misma serie.

En cuanto al software utilizado por este dispositivo de grabación de imágenes de CCTV, la página oficial de la marca menciona que todos sus dispositivos utilizan el software **VideoSphere**, el cual realiza las grabaciones con

un formato **mpg** y se pueden obtener en formato **jpg** si se cuenta con el software adicional, ninguno de estos dos formatos corresponde al formato entregado por la institución bancaria.

Las imágenes entregadas por la institución bancaria fueron en formato .ppt, el cual corresponde al software de Microsoft Office conocido como Power Point.

La página oficial de la marca MARCH es: http://www.marchnetworks.com/

19) Explicar cuáles son las funciones del programa Team Viewer y otros similares y dictaminar si alguno de ellos se encuentra instalado en los equipos involucrados o cualesquiera otro de la sucursal, y, en su caso obtener los archivos de registro de su utilización explicitando las fechas y las horas en que fue activado.

Respuesta:

TeamViewer es una aplicación de escritorio remoto que permite a quien la ejecute el poder establecer conexión y administración de recursos sin necesidad de estar físicamente en la computadora donde se encuentra instalada la aplicación correspondiente, ni que sea necesario que las operaciones que la aplicación permite realizar sean realizadas por la persona o personas legítimamente autorizadas para ello.

A partir del análisis forense que el perito realizó sobre la información contenida en los discos duros de los equipos de cómputo que ejecutan tanto el proceso cliente como el proceso servidor, de la aplicación de software cliente/servidor AS de la institución bancaria, se encontró, respecto a este punto del dictamen, lo siguiente:

1) En el disco duro del equipo de cómputo donde se ejecuta el proceso servidor, de la aplicación de software cliente/servidor AS, se encontró instalado la aplicación de software de nombre **NetView Dm/2**, la cual, de manera general, se puede decir que permite la comunicación de un servidor con otro, así como también permite la administración de software o aplicaciones de manera remota.

2) Esta aplicación **NetView Dm/2** realiza las mismas funcionalidades que la aplicación Team Viewer y otras similares.

3) Por medio de la aplicación **NetView Dm/2**, se pueden ejecutar las sesiones cliente (aplicaciones que usan los cajeros para realizar operaciones bancarias) que se deseen y realizar con ellas las mismas operaciones que realiza un cajero frente a ventanilla.

4) Por medio de la aplicación **NetView Dm/2**, las sesiones cliente y las operaciones bancarias mencionadas en el punto 3 anterior, se pueden realizar de manera remota por una persona distinta al cajero.

5) Lo descrito en los puntos 1, 2, 3 y 4 anteriores abre totalmente la posibilidad de que las operaciones fraudulentas imputadas a los inculpados hayan sido realizadas en realidad por medio de este software, desde la computadora que ejecuta el proceso servidor de la aplicación AS y por terceras personas distintas a los inculpados.

6) Al analizar los registros de bitácora (archivo MESSAGE.DAT) de la aplicación **NetView Dm/2***, existe un registro del día del incidente, es decir,

02/04/2008 (2 de Abril del 2008) que muestra la activación de esta aplicación **NetView Dm/2***, a las 04: 46:03. Este registro es el siguiente:

íí

**** NetView DM/2 logged at 04:46:03 02/04/2008 ****

ANX0131: (I) The file identified by Global Name 'GSCATCON.CAM' and Local Name

'C:\IBMNVDM2\FSDATA\FSF00007' has been updated.

íí

7) La fecha y hora de activación corresponde al 2 de Abril de 2008 a la cuatro horas, cuarenta y seis minutos, tres segundos de la mañana y no hay registro de baja de tal aplicación.

8) Después de los registros con fecha del 03/04/2008 (3 de Abril del 2008) los registros comienzan a aparecer con fecha de 01/01/1980 (1 de Enero de 1980), para reaparecer de nuevo con fecha del 4 y 5 de Abril de 2008.

9) Al parecer la secuencia de aparición en orden cronológico de los registros fue alterada o cambiada o bien pudieron haber sido borrados algunos registros justo en los rangos de fechas de ocurrencia del incidente.

10) Este comportamiento anómalo hace pensar que dichos registros pudieron ser modificados al saber que dichos registros contienen información de conexiones con el servidor, o tienen la capacidad de mostrar si se instaló alguna aplicación o software de forma remota, o si se instaló algún software malicioso, o si hubiese existido alguna conexión indebida al servidor.