Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela Ingeniería de Sistemas

Tema:

Análisis del fraude Informático en la Importadora “CERIMCOVA” Cia. Ltda., cometido en Septiembre del 2008

Diseño de Monografía previo a la obtención del título de Ingeniería de Sistema

Autor (es):

Córdova Valverde Andrés Esteban

Piedra Domínguez Paul Esteban

Director:

Ing. Diego Condo D.

Cuenca, Ecuador

2009

DEDICATORIA I

Dedico esta monografía a mi familia y amistades las cuales me ayudaron con su apoyo incondicional a ampliar mis conocimientos y estar más cerca de mis metas profesionales. Esto fue posible primero que nadie con la ayuda de Dios, gracias por otorgarme la sabiduría y la salud para lograrlo. Dios los bendiga!!!

Andrés Córdova Valverde

DEDICATORIA II

Quiero dedicarle este trabajo, A Dios que me ha dado la vida y fortaleza para terminar este proyecto de investigación, A mis Padres por estar ahí cuando más los necesité y ayudarme en los momentos más difíciles.

Esteban Piedra Domínguez

AGRADECIMIENTO

Agradecemos sobre todo a Dios, a nuestros padres que nos dieron todo su apoyo para poder progresar, gracias por estar con nosotros en todas las ocasiones de nuestras vidas y a nuestro director de monografía por su apoyo y tiempo empleado para sacar adelante esta monografía y por las enseñanzas que nos brindo para salir adelante.

Andrés Córdova Valverde
Esteban Piedra Domínguez

INDICE DE CONTENIDOS

RESUMEN

El valor de la información en nuestra sociedad, y sobre todo en las empresas, es cada vez mas importante para el desarrollo de cualquier organización, basándonos en el fraude cometido en la Importadora CERIMCOVA Cía. Ltda., una empresa familiar constituida de hecho, con la finalidad de que sirva como respuesta a problemas de privacidad, competencia desleal, robo de información confidencial y el objetivo de esta monografía es realizar un peritaje utilizado una metodología técnica especializada y de conformidad a la ley, siguiendo cada momento los principios fundamentales de la información forense, documentando totalmente y a fondo el proceso investigativo, utilizado herramientas hardware adecuadas y herramientas software forenses especializadas..

ABSTRACT

The value of information in out society, and above all for businness, is becoming more and more important for the development of any organization. Base don the fraud committed in the Importer CERIMCOVA Cia. Ltda., a family business created to serve as an answer to the problems of privacy, disloyal competition an theft of confidential information, the object of this monograph is to do an analysis using a specialized technical methodology and in conformity with the law. It will be done following the fundamental principals of forensic information at every step, completely documented, using adequate harware and specialized fofrensic software tolos used at the heart of the investigative process.

Introducción

Debido a que en nuestro medio existen empresas afectadas por la falta de políticas como es el caso de la “Importadora CORVAL Cía. Ltda.” Integrada en enero del 2002 por: Juan Carlos Córdova, Cesar Córdova, Milton Córdova, Mauricio Leser y Carlos Cornejo; la misma que se constituyo como una compañía de hecho, su ubicación es en la ciudad de Cuenca, ave. 12 de Abril y Unidad Nacional, y que su principal actividad es la venta de productos exclusivos en acabados de construcción entre los que destacan: cerámica, porcelanato, tinas, griferías, etc.

Con el objetivo de identificar y afirmar las sospechas de los Directivos se ha propuesto a indagar y recopilar la información necesaria que se encuentra en el sistema informático, sistemas periféricos y demás medios.

Determinando el medio de evidencia después de indagar las funciones, opciones del sistema y tipo de información que manejaban los funcionarios de los departamentos, profundizaremos en el análisis del software de la importadora para conocer concretamente el alcance de estas opciones y tipo de información que pueden aclararnos como pudo haberse fugado la información de carácter confidencial de “CERIMCOVA”.

Realizando el proceso en dos partes, la primera parte se centra en verificar respecto al ingreso de la información a la aplicación de Sistema de Facturación en la base de datos de Visual Fox Pro para consultar información relativa a clientes, proveedores y artículos por el año 2008, y la segunda parte se centra en la verificación acerca de la existencia, borrado o destrucción de archivos tipo Excel relacionados con la consulta.

Y presentar un informe Judicial en el que se indica las personas que están involucradas, auditores y testigos y además se detalla detenidamente todo el proceso de la recolección de evidencias con las herramientas adecuadas e indicando las mismas con sus versiones y los tiempos de ejecución de los procesos y además detallando los archivos encontrados con sus respectivas fechas e indicando finalmente como conclusión lo que se ha observado.

Capítulo I

Análisis de la Importadora CERIMCOVA CIA. LTDA.

1.1 Conocimiento de Empresa

En enero del 2002 se creó la "Importadora CORVAL Cía. Ltda." Integrada por: Juan Carlos Córdova, Cesar Córdova, Milton Córdova, Mauricio Leser y Carlos Cornejo; la misma que se constituyo como una compañía de hecho, su ubicación es en la ciudad de Cuenca, ave. 12 de Abril y Unidad Nacional.

Foto1.1- Importadora CERIMCOVA Cía. Ltda."

En el año 2007 por cuestiones de duplicidad en la razón social del negocio, esta importadora cambia su razón social por el de "Importadora CERIMCOVA Cía. Ltda." Teniendo como socios a todas las personas redactadas anteriormente excepto el ultimo.

La actividad principal de "Importadora CERIMCOVA Cía. Ltda." Es la venta de productos exclusivos en acabados de construcción entre los que destacan: cerámica, porcelanato, tinas, griferías, etc.

Foto1.2- Cenefas

Foto1.3- Baños completos

Foto1.4- Porcelanato

Foto1.5- Griferías

Foto1.6- Tinas-hidromasaje

Foto1.7- Piso flotante

La Importadora trabaja con proveedores de primerisimo nivel provenientes de Europa y Sur America por lo que se ha mantenido en el mercado hasta la fecha como una de las empresas en su linea vanguardista en sus productos, seria con sus proveedores y reconocidas ante sus clientes.

1.2 Objeto de Análisis

Desde su creación en “CERIMCOVA Cía. Ltda.” ha existido la armonía entre sus trabajadores lo cual se ha reflejado en el crecimiento de dicha empresa a lo largo de todo este tiempo.

A finales del mes de Julio y principios de Agosto del año 2008 esta armonía fue quebrantada debido a una fuerte pelea entre la Secretaria1 (llamaremos así para no revelar su identidad) y el Gerente General por cuestiones laborales y esto ocasionó un ambiente de trabajo “denso” a nivel de todo el personal provocando la renuncia irrevocable de la secretaria1 para inicios del mes de Septiembre. Evidentemente como toda labor de un Directivo es superar altos y bajos para mantener el orden y calidad en el funcionamiento de una empresa, el Gerente de “CERIMCOVA” aceptó la renuncia de la secretaria1 y reemplazo esa bacante con otra persona que la llamaremos secretaria2 a finales del mes de Septiembre del 2008.

A finales del mes de Noviembre del 2008 como de costumbre, la importadora “CERIMCOVA Cía. Ltda.” manteniendo las muy buenas relaciones comerciales con sus proveedores, llamo la atención a su Gerente una negociación en particular con uno de sus proveedores debido a que este último le exigía a “CERIMCOVA Cía. Ltda.” un aumento en el volumen de compras debido a que hay otra Empresa que

desea iniciar y mantener negocios, adquiriendo una mayor cantidad de los productos que son objeto de negociación con “CERIMCOVA Cía. Ltda.”.

En los meses de Noviembre, Diciembre del 2008 y Enero del 2009, los vendedores y la gente de almacén de “CERIMCOVA Cía. Ltda.” fueron llamados la atención por sus clientes en razón de informar que hay vendedores de la “otra Empresa” mencionada en el punto anterior, ofreciéndoles productos que eran exclusivos de “CERIMCOVA Cía. Ltda.” a menor precio.

Por lo redactado en los párrafos anteriores se observa que ha existido fuga de información propia de la empresa y esto se ha visto reflejado en el comportamiento de mercado en el que se maneja “CERIMCOVA Cía. Ltda.” a causa de las bajas en las ventas y perdidas en distribuciones exclusivas de ciertos productos.

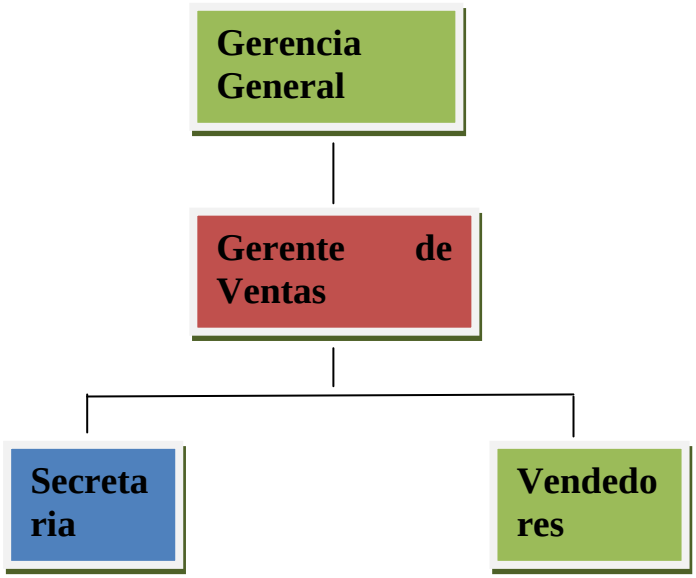
Para identificar y afirmar las sospechas de los Directivos se ha propuesto a indagar y recopilar la información necesaria que se encuentra en el sistema informático, sistemas periféricos y demás medios que permitan cumplir los objetivos propuestos en esta monografía.

1.3 Delimitación y análisis

Con el objeto de establecer la fuente o foco de filtración de la información vamos a analizar los diferentes departamentos o áreas con el objeto de delimitar las vulnerabilidades que presenta el sistema informático.

En este punto se procederá a conocer los diferentes departamentos y sus funcionarios que tienen acceso a la información para realizar las transacciones.

Grafico 1.- Esquema organizacional de CERIMCOVA en el que pudo haber fuga de información.



Departamento:	Gerencia General
Función:	Es la persona quien dirige, ejecuta, controla y toma decisiones acertadas para salvaguardar los intereses de la empresa; entre otras cosas es la encargada de mantener, buscar relaciones comerciales con los proveedores.
Accesos a módulos permitidos:	Inventarios, Compras, Ventas.
Principales Consultas y Reportes permitidos:	Detalle de artículos Detalles de Proveedores Detalles de Clientes
Opciones del sistema para generar reportes:	Guarda en formato .xls (Microsoft Excel). Imprimir en pantalla.

Departamento:	Gerente de Ventas
Función:	Es la persona que inspecciona las condiciones de ventas generadas así como el cobro de las mismas, juntamente con el trato y términos de negociaciones entre los vendedores y los clientes.
Accesos a módulos permitidos:	Inventarios, Compras, Ventas.
Principales Consultas permitidos:	Detalle de artículos Detalles de Proveedores Detalles de Clientes
Opciones del sistema para generar reportes:	Guarda en formato .xls (Microsoft Excel). Imprimir en pantalla.

Departamento:	Secretaria
Función:	Es un auxiliar contable y vendedor dentro de almacén.
Accesos a módulos permitidos:	Inventarios, Compras, Ventas.
Principales Consultas permitidos:	Detalle de artículos

	Detalles de Proveedores Detalles de Clientes
Opciones del sistema para generar reportes:	Guarda en formato .xls (Microsoft Excel). Imprimir en pantalla.

Departamento:	Vendedores
Función:	Son las personas que realizan las comercializaciones de los productos a los consumidores finales fuera del almacén.
Accesos a módulos permitidos:	Ninguno.
Principales Consultas permitidos:	Ninguno.
Opciones del sistema para generar reportes:	Ninguno.

Cabe anotar que cada funcionario de los distintos departamentos ingresa al sistema con un usuario y contraseña creados por el Jefe del Departamento de Sistemas.

Se conocerá detallada y gráficamente los módulos, consultas y reportes descritos en los cuadros por departamentos en el punto 1.4.

1.4 Determinación del medio de evidencia

Después de indagar las funciones, opciones del sistema y tipo de información que manejaban los funcionarios de los departamentos descritos en el punto 1.3 profundizaremos en el análisis del software de la importadora para conocer concretamente el alcance de estas opciones y tipo de información que pueden aclararnos como pudo haberse fugado la información de carácter confidencial de "CERIMCOVA".

A manera global vamos a describir las generalidades del sistema:

Sistema operativo en el que trabaja el sistema:	Windows Xp Home Service pack 2
Lenguaje en el que se desarrolló el sistema:	Visual Fox pro
Base de Datos que maneja el sistema:	Fox Pro
Usuarios que manejan el	Gerente General, Gerente de Ventas, Secretaria.

sistema:	
Módulos principales del sistema:	Inventarios, Compras, Ventas.
Parámetros Generales:	Parametrizable (de acuerdo a la situación económica, contable, fiscal actual) realizado por el Jefe del Departamento de Sistemas.

Podemos decir que este sistema lleva el control de clientes, proveedores, contabilidad, etc.; es decir registra y salvaguarda todas las transacciones comerciales que realiza la empresa el cual genera archivos en formato Excel.

A continuación describiremos y analizaremos los módulos principales del sistema con las diferentes opciones que estos manejan:

INVENTARIOS: dentro de este tenemos:

Líneas: es la clase mayor por la que se agrupa a los artículos.

Imagen 1.1- Ingreso a la opción de Líneas.

Esta opción emite un reporte tanto en impresora como en Excel de todas las líneas existentes

Imagen 1.2- Ingreso a la opción de imprimir Líneas.

Grupos: Es una subclase de líneas que especifica con más precisión a que grupo pertenece el articulo.

Esta opción emite un reporte tanto en impresora como en Excel de todos los grupos existentes pertenecientes a una línea.

Imagen 1.3- Ingreso a la opción de imprimir Grupos.

Artículo: es la descripción del producto a vender.

Imagen 1.4- Ingreso a la opción de Artículos.

Esta opción emite un reporte tanto en impresora como en Excel de todos los artículos existentes bajo ciertos criterios.

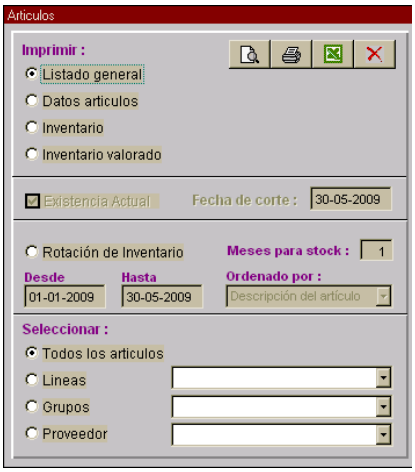


Imagen 1.5- Ingreso a la opción de generar reportes de artículos.

Destino: es el concepto del movimiento contable del artículo.

Esta opción emite un reporte tanto en impresora como en Excel de todos los destinos existentes que se le da al artículo.

Movimientos: son las transacciones contables de los artículos.

Esta opción emite un reporte tanto en impresora como en Excel de todos los movimientos transaccionales del artículo.

Kardex: es el historial de todos los movimientos del artículo.

Esta opción emite un reporte tanto en impresora como en Excel del kardex del artículo.

Toma física: ingreso del stock de cada artículo.

Esta opción emite un reporte tanto en impresora como en Excel del stock del artículo.

COMPRAS: se encuentran aquí:

Proveedor: contiene todos los datos del proveedor.

Esta opción emite un reporte tanto en impresora como en Excel de los proveedores bajo ciertos criterios.

Imagen 1.6- Ingreso a la opción de Proveedores.

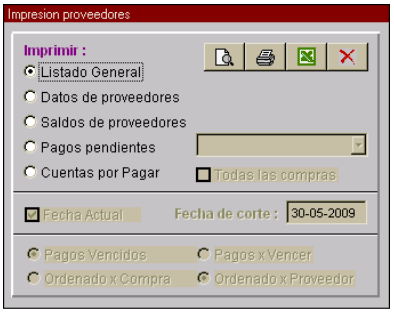


Imagen 1.7- Ingreso a la opción de generar reportes de proveedores.

Orden de compra: realiza una orden de compra al proveedor, es una pre factura.

Esta opción emite un reporte tanto en impresora como en Excel de las órdenes de compras que se hacen a los proveedores bajo ciertos criterios.

Compras: es la factura de compra, aquí se encuentran todos los artículos que realmente se van a adquirir.

Esta opción emite un reporte tanto en impresora como en Excel de las compras que se hacen a los proveedores bajo ciertos criterios.

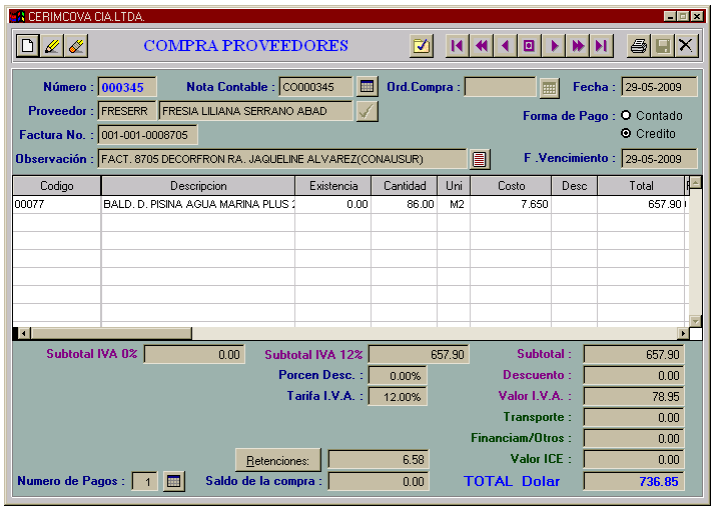


Imagen 1.8- Ingreso a la opción de Compras.

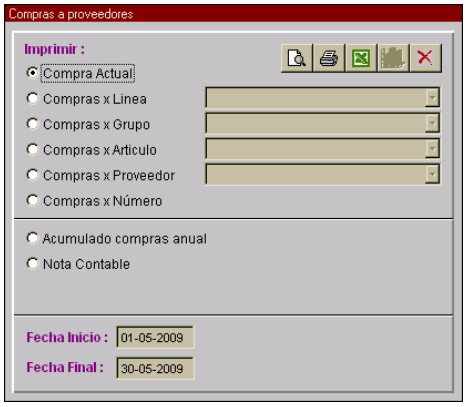


Imagen 1.9- Ingreso a la opción de generar reportes de compras a proveedores.

Servicios: aquí se registra todos los servicios que se realizaron para comprar al proveedor, estos no afectan o no se registran al inventario.

Esta opción emite un reporte tanto en impresora como en Excel de los servicios al proveedor.

Pagos: describe las cancelaciones de dinero por deuda con los proveedores.

Esta opción emite un reporte tanto en impresora como en Excel de los pagos al proveedor bajo ciertos criterios.

Débitos: es el ingreso de los créditos del proveedor.

Esta opción emite un reporte tanto en impresora como en Excel de los débitos que se le hacen al proveedor.

Estado de Cuenta: reporte de deudas con el proveedor.

Esta opción emite un reporte tanto en impresora como en Excel de los estados de cuenta del proveedor.

Historial: es el historial de las negociaciones con el proveedor.

Esta opción emite un reporte tanto en impresora como en Excel del historial del proveedor.

VENTAS: tenemos:

Clientes: contiene todos los datos de los clientes.

Esta opción emite un reporte tanto en impresora como en Excel del cliente bajo ciertos criterios.

Imagen 1.10- Ingreso a la opción de Clientes.

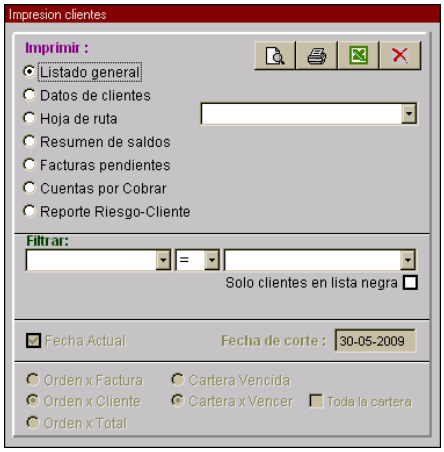


Imagen 1.11- Ingreso a la opción de generar reportes de clientes.

Proformas: cotización de los artículos pedida por los clientes.

Esta opción emite un reporte tanto en impresora como en Excel de las proformas para el cliente.

Pedidos: es más formal que la proforma pude ser una factura.

Esta opción emite un reporte tanto en impresora como en Excel de los pedidos realizados por el cliente bajo ciertos criterios.

Factura: documento final de la venta.

Esta opción emite un reporte tanto en impresora como en Excel de las facturas del cliente bajo ciertos criterios.

Abonos: ingreso de los pagos a las facturas de los clientes.

Esta opción emite un reporte tanto en impresora como en Excel de los abonos de las deudas del cliente.

Cartera: descripción de las facturas vencidas de los clientes.

Esta opción emite un reporte tanto en impresora como en Excel de cuanto se dispone de dinero en caja chica.

Vendedor: aquí se registra información de los vendedores tanto personal como del trabajo realizado.

Esta opción emite un reporte tanto en impresora como en Excel de los vendedores bajo ciertos criterios.

Imagen 1.12- Ingreso a la opción de Vendedores.

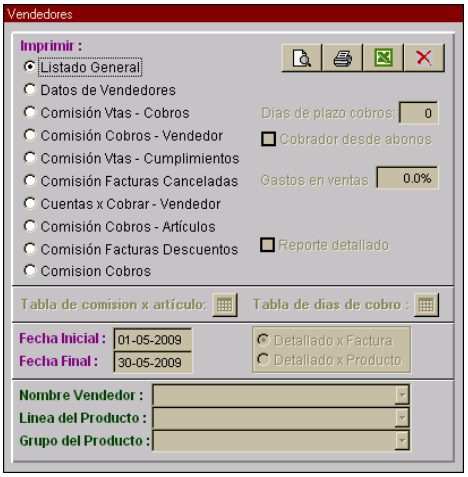


Imagen 1.13- Ingreso a la opción de generar reporte de vendedores.

Créditos: ingreso de los créditos a los clientes.

Esta opción emite un reporte tanto en impresora como en Excel de los créditos a los clientes.

Precios: descripción de los precios de los artículos para mayoristas, minoristas, lista de precios y costos, existencias, utilidad y rentabilidad.

Esta opción emite un reporte tanto en impresora como en Excel de los precios de minorista, mayorista, etc., que maneja CERIMCOVA.

Imagen 1.14- Ingreso a la opción de Precios.

Estado de cuenta: saldos pendientes de los clientes.

Esta opción emite un reporte tanto en impresora como en Excel del estado de cuenta del cliente.

Historial: aquí se registra el historial de negociaciones del cliente.

Esta opción emite un reporte tanto en impresora como en Excel del historial del cliente

Para tener una mejor idea de la estructura y funcionamiento en la que se basa todo el sistema de facturación de “CERIMCOVA” creemos que es necesario ilustrar con un Diagrama Entidad – Relación:

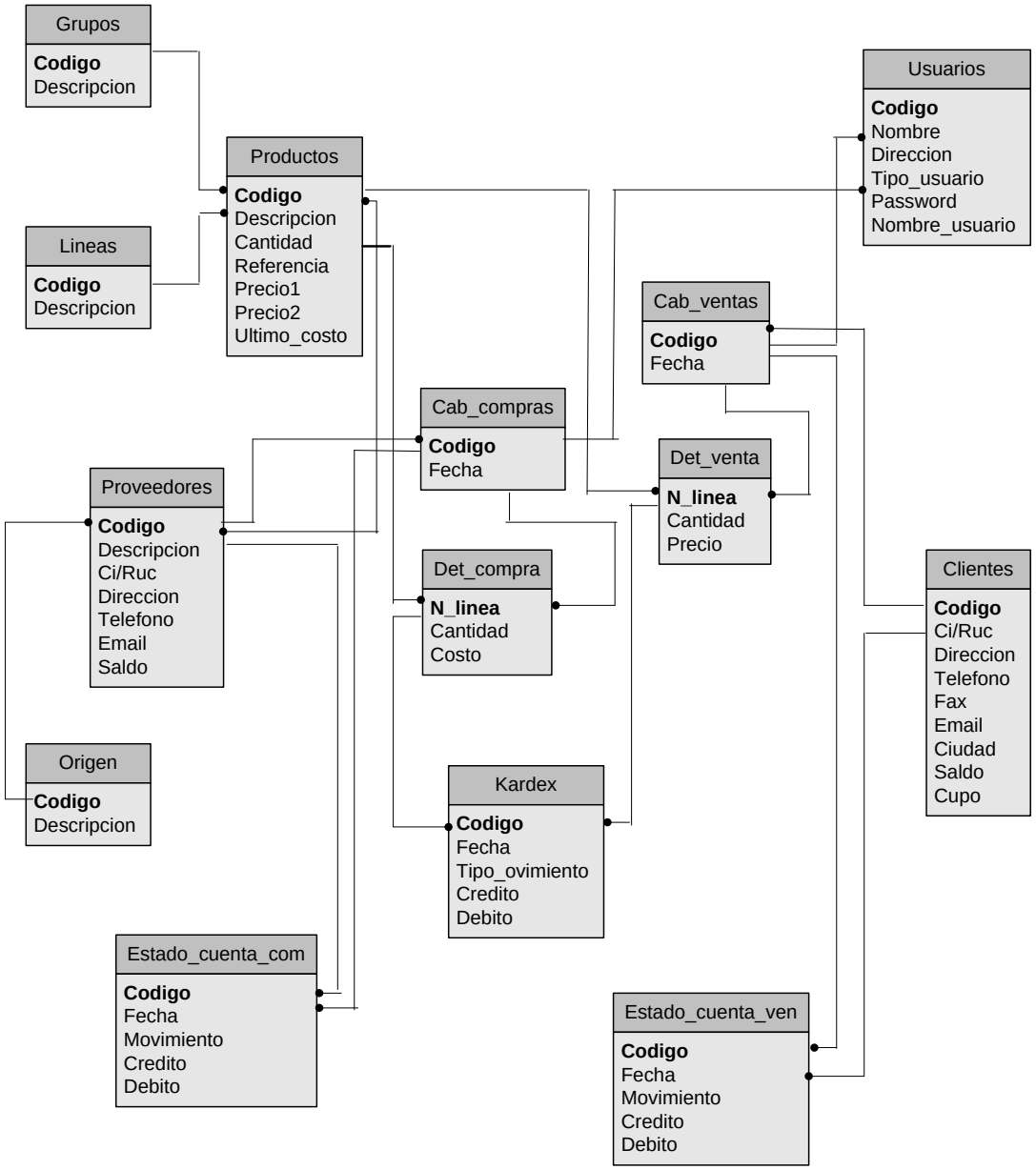


Imagen 1.15- Diagrama Entidad-Relación del Sistema de facturación de CERIMCOVA Cía. Ltda.

1.4.1 Dónde se encuentra la evidencia

Con los antecedentes de:

El conflicto dado con la secretaria1 y el Gerente General previo a su renuncia.

Los vendedores en los meses de Noviembre, Diciembre y Enero han observado y recibido comentarios de los clientes de que hay un proveedor local que ofrece el mismo portafolio de productos manejados por “CERIMCOVA” a menor costo produciendo una “competencia desleal” en el mercado que incursiona “CERIMCOVA’ por lo que se procedió a hacer reuniones con los directivos para analizar los motivos de las bajas en ventas.

Por lo analizado y realizado en el punto 1.3 y 1.4 podemos decir que las vulnerabilidades que el sistema presenta para que se haya dado una fuga de información se encuentra en el departamento de ventas (anexo 1 mapa empresa hecho en visio) donde sus funcionarios: Gerente de Ventas, Secretaria tienen los mismos accesos al sistema y por lo tanto manejan la misma información (Artículos, Proveedores, Clientes).

De los antecedentes descritos se determino como vulnerabilidad y objeto de análisis lo acciones del usuario "Secretaria 1" descartando al Gerente de Ventas por lo que es dueño accionista de la empresa y a los vendedores porque no tienen acceso al sistema de facturación.

Con lo descrito anteriormente la computadora que tenia instalado el sistema de facturación manejado por Usuario "Secretaria 1" (anexo2 acta e/r) y donde posiblemente se encuentre la evidencia es una computadora con las siguientes características:

Tipo de Computadora:	Clon
Marca:	Mega Clon
Tipo y Capacidad de Procesador:	Intel Celeron de 2.8 Ghz.
Capacidad de Memoria Ram:	225 M.B.
Capacidad de almacenamiento:	80 G.B.

Foto1.8 y 1.9- Computadora de "Secretaria 1"

1.4.2 Cómo se encuentra almacenada la evidencia

En base al estudio realizado en los puntos anteriores podemos decir que la información de: Artículos, Proveedores y Clientes pudo haber sido extraída en archivos tipo Excel con la extensión ".xls" en un rango de fechas entre Mayo y Septiembre del 2008 y la persona quien realizó esto se demostrará y comprobará con los log's de acceso a la Base de Datos ya que cada funcionario del departamento de Ventas cuenta con usuario y contraseña.

1.5 Fundamentos de derecho (Marco Legal Ecuatoriano)

El sustento legal del presente trabajo se sustenta en el Marco Legal Ecuatoriano:

Revisión Legal:

Constitución Política del Ecuador

Código de Procedimiento Penal

Comercio Electrónico y Firma Digital

Otras Normativas.

Esto punto lo profundizaremos a continuación en el capítulo 2.

Conclusión Capitulo I:

Podemos decir que la “Importadora CERIMCOVA Cía. Ltda.” es una empresa joven integrada por familiares que ha logrado confiabilidad y prestigio a través de los años que lleva en el mercado debido a la exclusividad en sus productos y clientes.

Competitivamente hablando esta opera en un entorno relativamente estable, el sector de la comercialización es sumamente competitivo, entre los principales competidores esta Importadora Vega, Boyaca, etc., los cuales aprovechan permanentemente todas las oportunidades a su alcance para tomar la delantera. Sin embargo, CERIMCOVA se ha mantenido debido al servicio que brinda a sus clientes.

Revisando y analizando todo lo investigado en el capítulo 1 podemos llegar a la conclusión que se determino como vulnerabilidad y objeto de estudio los movimientos o acciones del usuario “Secretaria 1” concretamente una fuga de información privada de “CERIMCOVA Cía. Ltda.” Indicando que es la más factible para realizar estas acciones ya que tenia accesos a la información de Artículos, Proveedores y Clientes, evidenciándose una falta total de normas de Control Interno en la empresa que es objeto de nuestra auditoria.

Esta información pudo haber sido generada en un archivo tipo Excel y después haber sido utilizada con fines perjudiciales para “CERIMCOVA” lo que se constituiría como la respuesta esperada a las sospechas de los Directivos de la Importadora.

Capítulo II

Fundamento Teórico

2.1 Aspectos Preliminares

Cuando en la ejecución de labores de auditoría (financiera, de gestión, informática, tributaria, ambiental, gubernamental) se detecten fraudes financieros significativos; y, se deba (obligatorio) o desee (opcional) profundizar sobre ellos se está incursionando en la denominada auditoría forense.

La investigación será obligatoria dependiendo de:

1) el tipo de fraude;

2) el entorno en el que fue cometido; y,

3) la legislación aplicable.

La labor de auditoría forense también puede iniciar directamente sin necesidad de una auditoría previa de otra clase, por ejemplo en el caso de existir denuncias específicas.

La auditoría forense es aquella labor de auditoría que se enfoca en la prevención y detección del fraude; por ello, generalmente los resultados del trabajo del auditor forense son puestos a consideración de la justicia, que se encargará de analizar, juzgar y sentenciar los delitos cometidos (corrupción financiera, pública o privada).

2.1.1 Etimología

Forense:

Perteneciente o relativo al Foro, a la Justicia.

Añádase por antonomasia a las ciencias que estudian las Evidencias para procesos judiciales.

Bases:

La Pericia Informática Forense se basa en Ciencias tales como:

Arqueología
Medicina
Geología
Criminalística
Electrónica
Telecomunicaciones
Derecho

Otras definiciones son:

"La Auditoria forense es el uso de técnicas de investigación criminalística, integradas con la contabilidad, conocimientos jurídico-procesales, y con habilidades en finanzas y de negocio, para manifestar información y opiniones, como pruebas en los tribunales. El análisis resultante además de poder usarse en los tribunales, puede servir para resolver las disputas de diversas índoles, sin llegar a sede jurisdiccional."

Pedro Miguel Lollett R. CFE

http://auditoriaforense.net/index.php?option=com_content&task=view&id=25&Itemid=39

"Es una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas y privadas".

Miguel Cano

http://auditoriaforense.net/index.php?option=com_content&task=view&id=25&Itemid=39

"La Auditoría Forense en la actualidad es reconocida internacionalmente como un conjunto de técnicas efectivas para la prevención e identificación de actos irregulares de fraude y corrupción."

Pablo Fudim

http://auditoriaforense.net/index.php?option=com_content&task=view&id=25&Itemid=39

"La auditoría forense es aquella labor de auditoría que se enfoca en la prevención y detección del fraude financiero; por ello, generalmente los resultados del trabajo del auditor forense son puestos a consideración de la justicia, que se encargará de analizar, juzgar y sentenciar los delitos cometidos (corrupción financiera, pública o privada)."

Jorge Badillo

http://auditoriaforense.net/index.php?option=com_content&task=view&id=25&Itemid=39

2.1.2 Definiciones

Perito:

"Persona idónea y/o profesional dotada de conocimientos y habilidades especializadas, que suministra información u opinión fundada sobre los puntos de su ámbito científico"[1].

Ciencia Forense:

2Aplicación de prácticas científicas dentro del proceso legal, con el objeto de proporcionar opinión fundada sobre un tema a los responsables de administrar Justicia"[2].

[1] **Pedro Miguel Lollett R. CFE Auditoria Forense**
[2] **Pedro Miguel Lollett R. CFE Auditoria Forense**

Evidencia:

"Certeza clara, manifiesta y tan perceptible, que nadie puede racionalmente dudar de ella. Toda prueba obtenida conforme a Ley"[3].

Prueba Pericial

"La prueba pericial es el medio por el cual personas ajenas a las partes, que poseen conocimientos especiales en alguna ciencia, arte o profesión y que han sido precisamente designadas en un proceso determinado, perciben, verifican hechos y los ponen en conocimiento del juez, y dan su opinión fundada sobre la interpretación y apreciación de los mismos, a fin de formar la convicción del magistrado, siempre que para ellos se requieran esos conocimientos. "[4].

Auditoria Forense

Se define inicialmente a la auditoría forense como una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas y privadas.

Auditoría Forense en la Investigación Criminal del Lavado de Dinero y Activos presenta la siguiente definición:[5].

Peritaje Informático Forense

"Proceso de Identificación, Adquisición, Preservación, Análisis y Presentación de Evidencia Digital, de acuerdo a Procedimientos Técnico-Legales preestablecidos, como apoyo a la Administración de Justicia en la resolución de un caso Legal". [6].

Evidencia Digital

Toda información digitalizada en formato electrónico susceptible de ser analizada por un método técnico y de generar conclusiones irrefutables en lo legal.

La EVIDENCIA DIGITAL es solamente la información contenida en un medio, que refleja el resultado de una operación informática, o capturada de un proceso de transferencia.

"Es una forma de Evidencia Física, construida por campos magnéticos y pulsos electrónicos, que pueden ser recolectados y analizados con herramientas y técnicas especiales"[7]

[3] **Pedro Miguel Lollett R. CFE Auditoria Forense**
[4] **Pedro Miguel Lollett R. CFE Auditoria Forense**
[5] **Pedro Miguel Lollett R. CFE Auditoria Forense**
[6] **Pedro Miguel Lollett R. CFE Auditoria Forense**
[7] **Pedro Miguel Lollett R. CFE Auditoria Forense**

Medio de Evidencia:

Los Medios Originales que contienen la Evidencia Digital a Investigar.

Imagen de Evidencia:

Copia del Medio de Evidencia utilizada para realizar el Análisis Forense, por clonación o método seguro.

Evidencia Volátil:

Aquella que no se encuentra preservada en un Medio, sino debe ser "congelada" mediante Herramientas adecuadas, en la Escena del Crimen.

Escena del Crimen

Es el espacio físico o virtual donde se cometio un delito y sus consecuencias, y que debe ser aislado para evitar la contaminación de la Evidencia antes de su correcta preservación.

Medio de Evidencia Digital

Son todos los Dispositivo físico que permite almacenar información digitalizada electrónicamente, en forma temporal o permanente, y que puede ser manejado de acuerdo a los procedimientos para Evidencia Física.

2.1.3 Objetivo

Se hace un Peritaje Informático para determinar QUE, COMO sucedió y QUIEN es responsable utilizando Metodología técnica y con conformidad de la Ley.

2.1.4 Etapas Fundamentales

En las etapas fundamentales para la Pericia Informática Forense se desarrolla en 4 etapas básicas:

A. Identificación y Adquisición
B. Preservación
C. Análisis Forense
D. Presentación Judicial

Además se tienen 4 Pasos que los enumeraremos

- dentificando la Evidencia Digital
- Preservando la Evidencia Digital
- Se debe ser capaz de llevar la cuenta de cada cambio realizado.
- Se Extraer para obtener información humanamente legible o irreproducible de un medio, se procesa para convertirla en información y se interpreta para comprensión más profunda de cómo se dieron las cosas.

2.1.5 Principios Fundamentales

Preserve la evidencia digital en su estado Original (sin cambios),

Documente totalmente (y a fondo) el proceso investigativo, trabajar siempre sobre copias idénticas de la Evidencia Original (clones), siempre con Herramientas adecuadas, No arriesgue su tiempo y la Evidencia del Cliente.

Nunca se debe de alterar las fechas, ni matar o terminar procesos al azar para hacer espacio en disco, parchar el Sistema antes de la Investigación, Ejecute Comandos en el Sistema sin registrar o documentar, Usar Comandos y Programas inseguros, instalar Software sobre el medio de la Evidencia y correr o ejecutar programas que almacenen temporales o salidas sobre el medio de la Evidencia.

2.2 Identificación y Adquisición

2.2.1 Definición

Es el hecho de identificar las pruebas que pueden encontrarse en el lugar en donde se dio el delito y el hecho de adquirir es la forma mas adecuada de obtener la evidencia sin ser corrompida o manipulada indebidamente.

2.2.2 Limitación del espacio

Las limitaciones del espacio se dan al momento de realizar el análisis en donde se pudo realizar o ejecutar el delito y además así reduciendo el espacio de análisis y para evitar que se está realizando un estudio en el espacio no necesario.

2.2.3 Determinación de Fuentes de evidencia

Para determinar las fuentes de evidencia es primordial verificar que sistemas se están utilizando y que y enfocarse en lo que se está buscando

El auditor deberá considerar las características de la evidencia. Por lo general, mientras más bajo sea el nivel de determinación, mayor debe ser la seguridad que debe proporcionar la evidencia.

2.2.4 Características de la Evidencia

Las características de la evidencia reunidas por el auditor tienen que ser:

Relevante.-La evidencia es relevante cuando ayuda al que ve la evidencia y llega a una conclusión respecto a los objetivos específicos del caso.

Autentificable.- La evidencia es auténtica cuando es verdadera en todas sus características.

Verificable.- Es el requisito de la evidencia que permite que dos o más lleguen por separado a las mismas conclusiones, en iguales circunstancias.

Neutral.- Es el requisito que esté libre de prejuicios. Que no tenga el fin de acusar sino de apoyar un hecho muy indiferente de que o quien sea y no debe haber sido diseñado para apoyar intereses especiales.

2.2.5 Procedimientos Forenses

Es la metodología o los pasos a seguir para realizar un peritaje forense y levantar toda la evidencia necesaria para presentar con reglas a los juzgados demostrando el caso de fraude cometido.

2.3 La Evidencia Digital

2.3.1 Definición

La evidencia digital es toda evidencia que puede ser considerada física construida por campos magnéticos que pueden ser obtenidos y analizados con herramientas y técnicas especiales

2.3.2 Determinación de la evidencia

Para determinar la evidencia es importante tomar en cuenta las siguientes normas:

Demostrar con hechos y documentación que los procedimientos aplicados para recolectar y analizar los registros electrónicos son razonables y robustos.

Verificar y validar con pruebas que los resultados obtenidos luego de efectuar el análisis de los datos, son repetibles y verificables por un tercero especializado.

Auditar periódicamente los procedimientos de recolección y análisis de registros electrónicos, de tal manera que se procure cada vez mayor formalidad y detalles en los análisis efectuados.

Fortalecer las políticas, procesos y procedimientos de seguridad de la información asociados con el manejo de evidencia digital.

Procurar certificaciones profesionales y corporativas en temas relacionados con computación forense.

2.3.3 La Cadena de Custodia

La cadena de custodia es un procedimiento establecido por la normatividad jurídica, que tiene el propósito de garantizar la integridad, conservación e inalterabilidad de elementos materiales de prueba (evidencias físicas) entregados a los laboratorios criminalísticas o forenses por la autoridad competentes, para el análisis de los mismos.

Principios Básicos de la Cadena de Custodia

- La cadena de custodia es un proceso organizado que está conformado por los funcionarios y personas, bajo cuya responsabilidad se encuentran las evidencias correspondientes, durante las diferentes etapas del proceso penal.

Es decir, todo funcionario que genere, reciba en custodia o analice muestras o elementos de prueba y documentos, forma parte de la cadena de custodia

- El Fiscal es responsable de probar que la Evidencia que se presenta en la Corte es la que se Preservó originalmente.
- Se debe mantener una Cadena de Custodia
- Crear una Etiqueta de Evidencia al momento de Preservarla
- Un Formulario de Cadena de Custodia que debe de contener toda la información necesaria para identificar los sucesos y asociar al caso.

Fecha / Hora
Número de Caso
Número de Etiqueta de Evidencia
Descripción de la Evidencia
Recepción individual de la Evidencia (Fecha/Hora)
Cada vez que la Evidencia se mueve para su análisis, almacenamiento, devolución, presentación u otra etapa del proceso, se debe hacer constar en el formulario de Cadena de Custodia
Fecha / Hora de movimiento
Origen y Destino de la Evidencia
Nombre / Firma de Entrega/Recibe
Observaciones del estado de la Evidencia
Motivo del movimiento.

La cadena de custodia se inicia desde los mismos momentos en que se conoce el hecho y la autoridad correspondiente colecta los elementos de prueba, en el Sitio del Suceso o en el cadáver y finaliza en el Tribunal de la causa.

Los procedimientos de custodia deben aplicarse a todo elemento probatorio con materialidad, sea un cadáver, un documento o cualquier otro material físico. Esa misma protección y vigilancia se deben ejercer de manera idéntica sobre las actas y oficios que acompañan el material.

2.3.4 Documentación

Es importante todo plasmar en papel con formularios y bolígrafos llenados a mano indicando la hora de inicio y fin en todas las paginas y indicando observaciones.

2.3.5 Preservación de la Evidencia: Volátil y no Volátil

Para la preservación de la evidencia es indispensable de un Laboratorio Forense Portátil que incluyen tanto Hardware como Software.

Hardware

Laptop con Booteo en Windows y Linux (Básico)
Adaptadores USB a 802.11x, 802.15, etc.
Racks SATA, IDE y SCSI
Buses para todo tipo de Conectividad a Disco.
Discos Duros de gran capacidad (para Imágenes).
Juego de Herramientas para Desarmar Hardware.

Software

dd, y otras formas de FDisks y manejadores de Particiones y File Systems
The Coroner's Toolkit, especialmente unrm, o equipo de Herramientas similar (Helix, Encase, FTK, etc.)
Soporte para TODOS los tipos de File Systems
Copias seguras de herramientas comunes (dd, cp, strings, ls, ps, netstat, ifconfig, lsof...) para todo tipo de plataformas.
Ayudas impresas para diferentes tipos de F.S.
Herramientas para Monitoreo de Red (netstat, Cain, GFIs, etc.)
Herramientas para Acceso y Control Remoto.

2.4 Análisis Forense

2.4.1 Procedimiento Previo

Para el análisis forense es importante tener un proceso previo verificando:

- El contenedor
- Los Sellos
- La Cadena de Custodia
- Fechas y Tiempos
- TODO DEBIDAMENTE DOCUMENTADO

2.4.2 Técnicas de Análisis

Para las técnicas de Análisis es importante identificar que busco, en donde tengo que buscar, como buscar y con que busco, ya que si se estos pasos es una buena técnica de análisis.

2.4.3 Procedimientos de Búsqueda

Son todos los pasos para la búsqueda de evidencia, es importante tener cuidado para realizar este tipo de búsquedas en no instalar ningún software en el equipo ya que puede eliminar evidencia que ha sido borrada, para recuperar con herramientas adecuadas, lo primero es enfocarse en lo que se está buscando y qué tipo de información se desea obtener.

2.4.4 Análisis de Herramientas

Para el análisis de herramientas es para verificar que tipo de herramientas se pudo utilizar para ocultar o eliminar la información del equipo para evitar que quedara evidencia en el equipo.

2.5 Presentación Judicial

En lo que se refiere a la presentación Judicial se realiza un informe en el que se indica las personas que están involucradas, auditores y testigos y además se detalla detenidamente todo el proceso de la recolección de evidencias con las herramientas adecuadas e indicando las mismas con sus versiones y los tiempos de ejecución de los procesos y además detallando los archivos encontrados con sus respectivas fechas e indicando finalmente como conclusión lo que se ha observado.

2.5.1 Objetivo

El objetivo principal es realizar un documento que se entienda y sea totalmente claro y con explicaciones que sea legible y que tenga explicación de cómo se obtuvo y se trato la información como lo detallamos en el CAPITULO III.

2.5.2 Descripción del Proceso

Es importante describir en el informe el proceso completo para realizar el peritaje informático como lo demostramos en el CAPITULO III.

2.5.3 Proceso de la Obtención de la Prueba

El proceso de obtención de la prueba depende de el lugar y el tiempo disponible como hemos mencionado en el presente capitulo y como lo describimos o mostramos como ejemplo en el CAPITULO III.

2.5.4 Proceso de Estudio de las Pruebas Obtenidas

Como hemos revisado en el capítulo se puede ver que para el proceso de estudio de las pruebas se tiene varias formas para el cual nosotros lo demostramos en el CAPITULO III.

2.5.5 Análisis de la Prueba Pericial

Para el análisis de las pruebas nos sustentamos en las normativas de analisis

2.5.6 Anexos y Sustento Legal

Es importante agregar anexos que contengan cartas, bitácoras y todo documento relacionado con el peritaje para que quede como un sustento legal de lo realizado para que quede todo transparente y entendible.

6 Marco Legal Ecuatoriano

2.6.1 Revisión Legal: Constitución Política del Ecuador

Entre los bienes jurídicos reconocidos en nuestra constitución política está la información.

DELITO INFORMATICO

CONDUCTA TIPICA, ANTIJURIDICA Y CULPABLE COMETIDA UTILIZANDO MEDIOS TECNOLOGICOS DE PROCESAMIENTO AUTOMATICO DE INFORMACION; O CONTRA LA INFORMACION PROCESADA AUTOMATICAMENTE Y EL SOPORTE LOGICO DE LOS ORDENADORES.”

CARACTERISTICAS DEL DELITO INFORMATICO

- Se origina en la existencia de tecnología de procesamiento automático de información.
- Es un delito en que generalmente se requieren conocimientos de computación.
- Son ilícitos difíciles de prueba.
- Efectos fácilmente son transnacionales pues los sistemas de información y comunicación son globales.
- Son delitos que causan graves daños en la sociedad en casi todos los bienes jurídicos tutelados por el estado.
- Son delitos que tienen una gran incidencia en lo económico.
- Requieren de un dolo específico contra el soporte lógico y la información procesada automáticamente o contra otros bienes jurídicos a través del uso de tecnologías de la información.

2.6.2 Código de Procedimiento Penal

DELITOS INFORMATICOS RECONOCIDO POR LA ONU

Fraudes cometidos mediante manipulación de computadoras.

Manipulación de datos de entrada.

Manipulación de programas

Manipulación de datos de salida:

- tarjetas de crédito: número de cuenta, panel para firma y banda magnética.

- Fraude por manipulación informática

2.6.3 Comercio Electrónico y Firma Digital

Según el ART. 58 de la ley de comercio electrónico en el código penal libro II "delitos en particular" titulo II "delitos contra las garantías constitucionales y la igualdad racial" capitulo V "delitos contra la inviolabilidad del secreto" indica que la obtención y utilización no autorizada de información de la o las personas que hayan obtenido información de datos personales para cederla, publicarla, utilizarla o transferirla sin autorización del titular tendrán prisión de 2 meses a 2 años multa 1000 a 2000 usd.

2.6.4 Ley de Régimen Tributario Interno

Art. 243.- Diligencia de inspección.- El funcionario responsable del proceso de determinación podrá efectuar la inspección y verificación de los registros contables, procesos y sistemas relacionados con temas tributarios, así como de sus respectivos soportes y archivos, tanto físicos como magnéticos, en el domicilio fiscal del sujeto pasivo o en el lugar donde mantenga tal información. También podrá realizar inspecciones y revisiones a los sistemas informáticos que manejen información --|-relacionada con aspectos contables y/o tributarios, utilizados por el contribuyente, y obtener, en medio magnético o impreso, los respaldos que considere pertinentes para fines de control tributario. Para ejecutar las diligencias de inspección, el funcionario responsable del proceso de determinación podrá acudir a las mismas acompañado de un equipo de trabajo multidisciplinario, de acuerdo a la finalidad de cada proceso. Una vez que se haya revisado y analizado la información, procesos, sistemas y demás documentos pertinentes se elaborará un acta en la que sentará razón de la culminación de dicha inspección y de la información analizada; esta acta será firmada, en dos ejemplares, tanto por el funcionario responsable del proceso de determinación como por el sujeto pasivo o por su representante debidamente autorizado, y por el contador general, de ser el caso; uno de los ejemplares del acta se entregará al sujeto pasivo y otro se agregará al expediente del proceso de determinación.

Art. 344.- Casos de **defraudación**.- (Sustituido por el Art. 31 de la Ley s/n, R.O. 242-3S, 29-XII-2007).- A más de los establecidos en otras leyes tributarias, son casos de defraudación:

1.- Destrucción, ocultación o alteración dolosas de sellos de clausura o de incautación;

2.- Realizar actividades en un establecimiento a sabiendas de que se encuentre clausurado;
3.- Imprimir y hacer uso doloso de comprobantes de venta o de retención que no hayan sido autorizados por la Administración Tributaria;
4.- Proporcionar, a sabiendas, a la Administración Tributaria información o declaración falsa o adulterada de mercaderías, cifras, datos, circunstancias o antecedentes que influyan en la determinación de la obligación tributaria, propia o de terceros; y, en general, la utilización en las declaraciones tributarias o en los informes que se suministren a la administración tributaria, de datos falsos, incompletos o desfigurados;
5.- La falsificación o alteración de permisos, guías, facturas, actas, marcas, etiquetas y cualquier otro documento de control de fabricación, consumo, transporte, importación y exportación de bienes gravados;
6.- La omisión dolosa de ingresos, la inclusión de costos, deducciones, rebajas o retenciones, inexistentes o superiores a los que procedan legalmente.
7.- La alteración dolosa, en perjuicio del acreedor tributario, de libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos;
8.- Llevar doble contabilidad deliberadamente, con distintos asientos en libros o registros informáticos, para el mismo negocio o actividad económica;
9.- La destrucción dolosa total o parcial, de los libros o registros informáticos de contabilidad u otros exigidos por las normas tributarias, o de los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias;
10.- Emitir o aceptar comprobantes de venta por operaciones inexistentes o cuyo monto no coincida con el correspondiente a la operación real;
11.- Extender a terceros el beneficio de un derecho a un subsidio, rebaja, exención o estímulo fiscal o beneficiarse sin derecho de los mismos;
12.- Simular uno o más actos o contratos para obtener o dar un beneficio de subsidio, rebaja, exención o estímulo fiscal;
13.- La falta de entrega deliberada, total o parcial, por parte de los agentes de retención o percepción, de los impuestos retenidos o percibidos, después de diez días de vencido el plazo establecido en la norma para hacerlo; y,
14.- El reconocimiento o la obtención indebida y dolosa de una devolución de tributos, intereses o multas, establecida así por acto firme o ejecutoriado de la administración tributaria o del órgano judicial competente.

Art. 345.- **Sanciones por defraudación**.- (Sustituido por el Art. 32 de la Ley s/n, R.O. 242-3S, 29-XII-2007).- Las penas aplicables al delito de defraudación son:

En los casos establecidos en los numerales 1 al 3 del artículo anterior y en los delitos de defraudación establecidos en otras leyes, prisión de uno a tres años.

En los casos establecidos en los numerales 4 al 12 del artículo anterior, prisión de dos a cinco años y una multa equivalente al valor de los impuestos que se evadieron o pretendieron evadir.

En los casos establecidos en los numeral 13 y 14 del artículo anterior, reclusión menor ordinaria de 3 a 6 años y multa equivalente al doble de los valores retenidos o percibidos que no hayan sido declarados y/o pagados o los valores que le hayan sido devueltos indebidamente.

En el caso de personas jurídicas, sociedades o cualquier otra entidad que, aunque carente de personería jurídica, constituya una unidad económica o un patrimonio independiente de la de sus miembros, la responsabilidad recae en su representante legal, contador, director financiero y demás personas que tengan a su cargo el control de la actividad económica de la empresa, sí se establece que su conducta ha sido dolosa.

En los casos en los que el agente de retención o agente de percepción sea una institución del Estado, los funcionarios encargados de la recaudación, declaración y entrega de los impuestos percibidos o retenidos al sujeto activo además de la pena de reclusión por la defraudación, sin perjuicio de que se configure un delito más grave, serán sancionados con la destitución y quedarán inhabilitados, de por vida, para ocupar cargos públicos.

La acción penal en los casos de defraudación tributaria tipificados en los numerales 4 al 14 del artículo anterior iniciará cuando en actos firmes o resoluciones ejecutoriadas de la administración tributaria o en sentencias judiciales ejecutoriadas se establezca la presunción de la comisión de una defraudación tributaria.

La administración tributaria deberá formular la denuncia cuando corresponda, en todo los casos de defraudación, y tendrá todos los derechos y facultades que el Código de Procedimiento Penal establece para el acusador particular.

2.6.5 Otras Normativas

ART. 14.- luego del art. 257.2 (aprovechamiento indebido de información reservada) agréguese el siguiente inciso:

Si el beneficio económico se obtiene por parte de la persona en razón de sus funciones, actividades, u oficios dentro del estado disponiendo de información, datos, archivos, documentos, programas (hardware y software), se aplicara la pena máxima. (Prisión 5 años)

Conclusión Capitulo II:

En este capítulo podemos concluir que se tienen muchos métodos para encontrar o demostrar que se ha cometido fraude o se intento cometer, mediante el análisis y obteniendo las pruebas periciales por medio de la evidencia, contando con herramientas adecuadas que permiten obtener las mismas de forma segura y que los datos no se modifiquen ya que es de suma importancia mantener la información intacta siempre y cuando se sigan las normas establecidas para realizar el análisis forense y para presentar un documento de informe lo mas claro y entendible posible para demostrar la culpabilidad o inocencia de acusado ante el juzgado siempre manteniendo distancia tanto con los implicados y mantener discreción y lo más importante que se tenga todo detallado en bitácoras de lo que se ha hecho y con testigos.

Capítulo III

Ejecución.- Análisis del fraude Informático en la Importadora "CERIMCOVA" Cía. Ltda., cometido en Septiembre del 2008

3.1 Aspectos Preliminares de fraude Informático en la Importadora

Para la realización del presente peritaje se ha utilizado una metodología técnica especializada y de conformidad a la ley, siguiendo cada momento los principios fundamentales de la información forense, documentando totalmente y a fondo el proceso investigativo, utilizado herramientas hardware adecuadas y herramientas software forenses especializadas.

Dado los hechos descritos en el capítulo 1 y el soporte técnico – teórico presente en el capítulo 2, en el presente capitulo llegaremos a indicios que son los que quedan supeditados a otros trabajos de peritaje o validación mediante presentación de pruebas de partes que apoyen o descarten los mismos. No generan una conclusión por si mismo, solo abren posibles líneas de investigación.

3.2 Identificación y Adquisición de la evidencia

Procederemos a indagar en el sistema de facturación de la compañía CERIMCOVA Cía. Ltda., que está instalado en la máquina de marca "clon" y que estaba a cargo de "*Secretaria 1*", con el objeto de realizar un análisis forense y así encontrar indicios que de constituirse en pruebas concretas y veraces servirá para que los Directivos de "CERIMCOVA" tomen las medidas correspondientes.

Para realizar esta tarea utilizaremos las siguientes herramientas:

- Helix v.1.8: Poderosa herramienta para realizar un análisis informático forense que permite sacar imágenes de cualquier dispositivo magnético de almacenamiento. Se la puede descargar gratis.
- Un disco duro externo de marca:"Maxtor" con la serie: 57212120414281DFZXX que se lo conectara en el puerto USB para almacenar la imagen que va a generar la herramienta Helix.

- Un disco duro externo de marca:"Maxtor" con la serie: 875152178236GFERW que se lo conectara en el puerto USB para almacenar la imagen que va a generar la herramienta Helix.

Ponemos a consideración la Bitácora de sucesos realizados del Viernes 1 al Domingo 3 de Mayo del 2009, adjuntando la cadena de custodia correspondiente (anexo 3).

Paso a1.- Aspectos Preliminares del Peritaje Informático

Llegada de los peritos quienes van a realizar la auditoría forense y el Sr. Moises Leser a la Importadora "CERIMCOVA Cía. Ltda.", donde se mantuvo una reunión en la que se manifestó por parte de los peritos al Señor Gerente, la técnica y procedimientos previo al análisis forense que se iba a realizar a la computadora en la que presuntamente se encuentra indicios en el estudio pericial de la evidencia, y que tiene las siguientes características:

Tipo de Computadora:	Clon
Marca:	Mega Clon
Tipo y Capacidad de Procesador:	Intel Celeron de 2.8 Ghz.
Capacidad de Memoria Ram:	225 M.B.
Capacidad de almacenamiento:	80 G.B.

Foto1.8 y 1.9- Computadora de "Secretaria 1"

Ubicada en el departamento de Ventas (anexo 3) y que estaba a cargo de "*Secretaria 1*" (anexo 4).

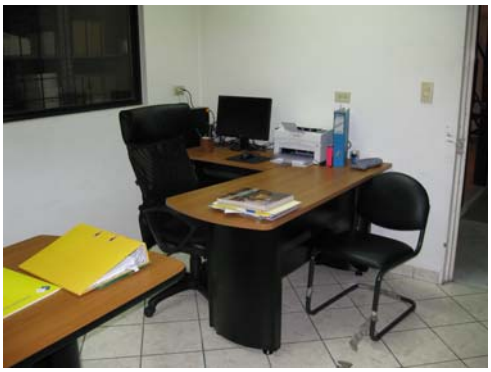


Foto3.1- Departamento de Ventas

Paso a2.- Comienzo del Análisis de la computadora de "*Secretaria 1*":

a2.1- Conocer la maquina partiendo del entorno de Windows:

Imagen 3.1- Escritorio de Windows.

a2.2- Conocer las características de la maquina:

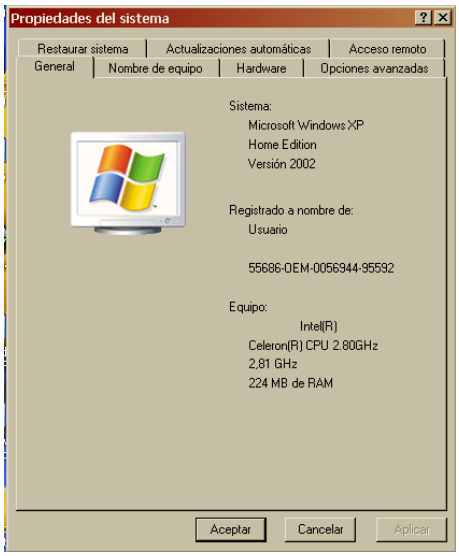


Imagen 3.2- Características de la computadora de "Secretaria 1".

a2.3 - Conocer las características de la red:

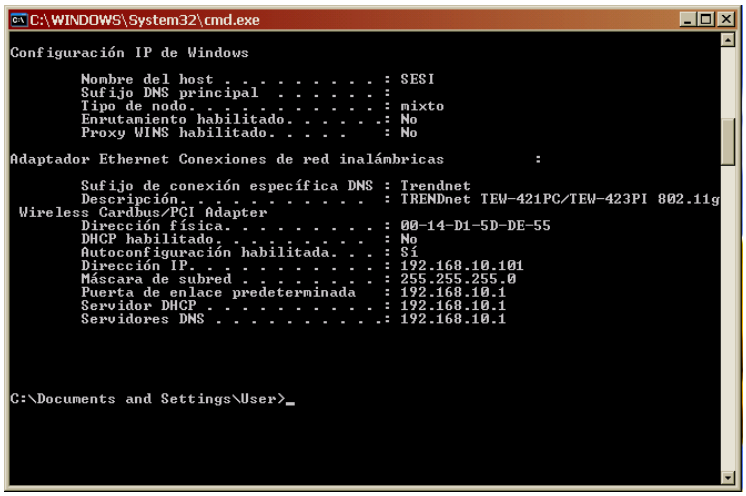


Imagen 3.3- Conocimiento del entorno de red.

a2.4 - Con la herramienta Helix v.1.8 se procede a obtener información del disco que va a ser objeto de análisis.

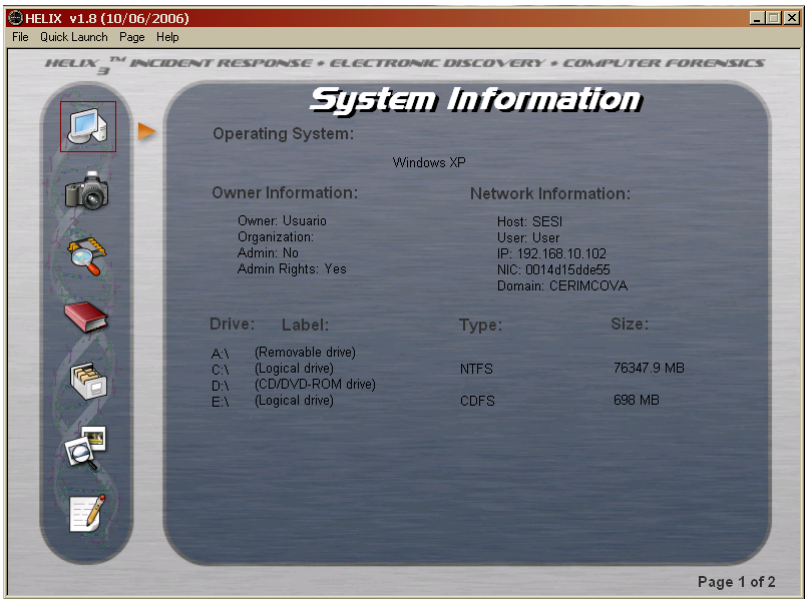


Imagen 3.4- Reconocimiento de Helix a la maquina donde se está aplicando esta herramienta.

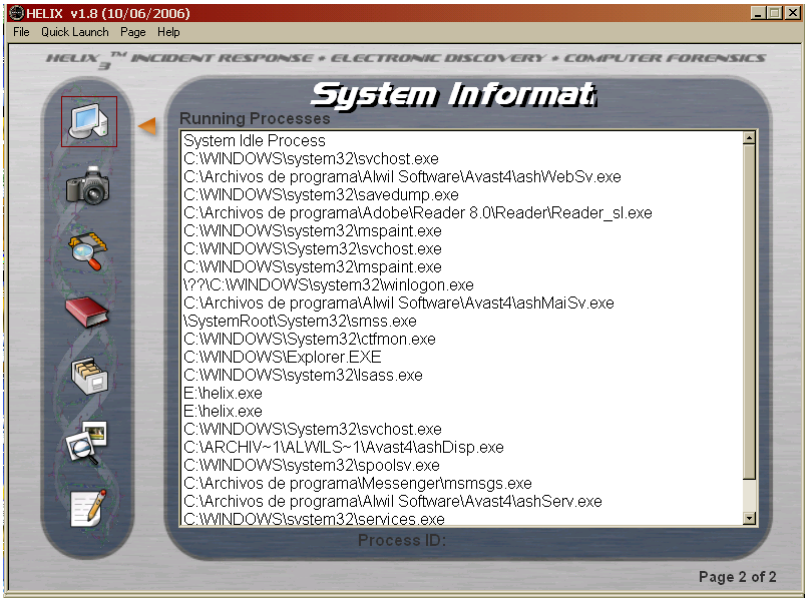


Imagen 3.5- Helix enlista todos los archivos actuales de la maquina.

Paso a3.- Obtención de las Imágenes de Disco con Helix

Procedimos los peritos a realizar el análisis forense en la maquina donde se encuentra indicios en el estudio pericial de la evidencia y lo primero que hicimos es utilizar la herramienta Helix con lo que se sacó dos imágenes y las almacenamos en

los respectivos discos duros externos conectados en el puerto USB de la mencionada computadora.

Con la segunda imagen no se trabajo, pero con la primera se realizó el análisis forense que describiremos a continuación:

Primera imagen obtenida:

Fecha y hora del Inicio del proceso	Viernes 1 de Mayo del 2009 21:11:40
Fecha y hora del Fin del proceso	Sábado 2 de Mayo del 2009 21:01:15
Archivo obtenido al finalizar el proceso	cerincova.dd, cerincova.dd_audit.log
Con un Hash numero	1570160389522466b42f603f6c5acbcc6761ab90
Archivo obtenido al finalizar el proceso	cerincova.dd.md5
Con un Hash numero	fd58aaaa40e3c88e8bb739d5fab8b53f
Almacenado en	disco duro externo de marca:”Maxtor” con la serie: 57212120414281DFZXX

Segunda imagen obtenida:

Fecha y hora del Inicio del proceso	Sábado 2 de Mayo del 2009 21:20:35
Fecha y hora del Fin del proceso	Domingo 3 de Mayo del 2009 21:40:37
Archivo obtenido al finalizar el proceso	cerincova.dd, cerincova.dd_audit.log
Con un Hash numero	1570160389522466b42f603f6c5acbcc6761ab90

Archivo obtenido al finalizar el proceso	cerincova.dd.md5
Con un Hash numero	fd58aaaa40e3c88e8bb739d5fab8b53f
Almacenado en	disco duro externo de marca:"Maxtor" con la serie: 875152178236GFERW

a3.1- Al finalizar el proceso de extracción de la primera imagen con el Helix, se obtuvo otro archivo llamado "reporte.xls" (donde se encuentra todos los archivos borrados del disco (anexo 4), ubicado en "F:\reporte.xls" y almacenado en el disco duro externo de marca:"Maxtor" con la serie: 57212120414281DFZXX

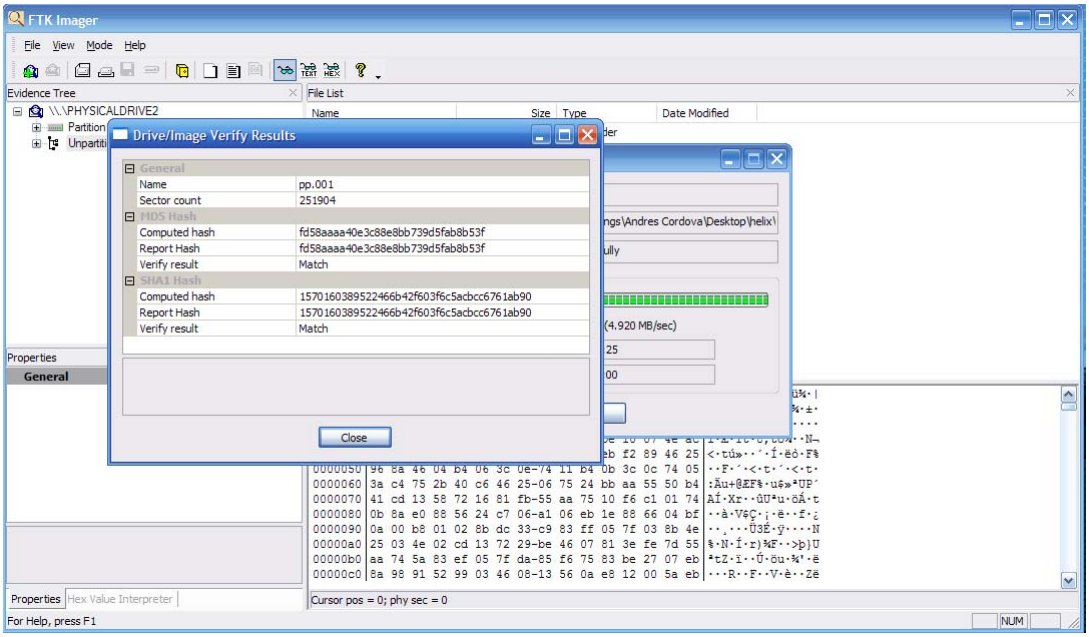


Imagen 3.6- Extracción y resultado de la imagen obtenida por Helix donde este saca entre otros archivos el numero de hash de la imagen del disco (cerincova.dd.md5) que se analizó.

3.3 La Evidencia Digital de la Importadora

Con el propósito de obtener indicios mediante presentación de pruebas que apoyen o descarten a los mismos, los peritos procedimos a analizar los resultados obtenidos en el punto 3.2 basándonos en el marco técnico – teórico descrito en el capítulo 2 (concretamente en el punto 2.5 Análisis forense)

El archivo “reporte.xls” tiene todos los archivos borrados en toda la existencia del disco, pero para nuestra investigación filtramos desde Julio a Septiembre del 2008 los archivos con extensión “.xls” donde se obtuvieron 56 archivos (anexo 4) que mostramos a continuación:

	MD5	SHA1	Filename
2	ad142e5e3a4d9d93a4a7859	aa0bcb03ce59b0acdb1fcace25a6	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\ACTA ENTREGA RECEPCION CONSORCIO.xls
3	0334adf08935429b25de6b9c	2ef3d08584301e15cd4cd3b23bc7	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\ADELCA.xls
4	9f7528e0b848aa1adb877bf6	d2c8e215f8f2f89b3e9d59d78f53	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\AIJIA #12.xls
5	3ca28870725dc3654e6a289e	2f14f9bbbf421a6fff787800874e2	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\AMORT.BCO. GUAYAQUIL JULIO08.xls
6	c2c9d9be4219204fd6d5b024	3b246493467f968f2794e5f5708e	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\AMORTIZACION VISA JUAN CORDOV.xls
7	551d2fb51bf61a0f83d0aace	2c356fb85c34bd547b57c580b33d	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\AMORTIZACION VISA JUAN CORDOVA.xls
8	e621c598355c2c7b5bb92535	cf64ac1eb24f87029e98360258e8	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\CHEQUES POSFECHADOS.xls
9	d4a23f792b06fd5eec130a82	f00a8a3be26470cce169474429f1	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\COLECCIONES CERAMICA AIJIA.xls
10	109da42b7ac97e93fbd73fc0	871bd51962dd03c7f3a890a2cf81	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\COTIZACION CARTA JULIO08.xls
11	c1a22cbbe7214380a4d3c3e5	177f4130290c27d063166906bd5e	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\cuadre de caja.xls
12	074367d77bdc8c1093470206	d85eba19b982ea1ee0de705dfc9	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\CURRICULUM MAESTRO CRIOLLO.xls
13	ebc2d5c44bf25f41e5c577c6	2111b078e8bae4b894084a5db56	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\DATOS CLIENTES.XLS
14	21a56c9a748c7fbab9f8a59d	ee2b77c47beca5cd4b2f68bbcf09	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\DECIMO CUARTO CERIMCOVA 08.xls
15	bc4c399e21aa17a96ba26e57	585ca84b640695b1a971bb2aa4e	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\DESCUENTO HORAS 08.xls
16	8771f97dc6e38b55d78ebb9	dd73286a2b100de6da8c811b5c4	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\FACT.AIJIA#10.xls
17	41ed352e67a48e3de00a0a6	0f6f528dea25e671b863ed9e6be	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\FACT.AIJIA#11.xls
18	a4b38f62bb05df9a56f5a6dc	74c81bf5376afadd849dfcd19dafc	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\flujo PAGO BCO INTER 2 AÑOS.xls
19	e96244be08f268828c26f861	6a5edabc1acb0d4d0fac17c821dc	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\FONDOS RESERVA CERIM08.xls
20	d60e72ed259ea3f51ccaba81	7ecd0520af5fdeeda5076633d83	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\LISTA DE PRECIOS ADELCA.xls
21	9ef9c998b38dc858629f528e	8b24daa1a0f1fd49d963c60d1bc4	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\LISTA DE PRECIOS ALFADOMUS.xls
22	d198d10413252e593ac8b44	f7f2019a99e6c09c38e6641116de	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\LISTA DE PRECIOS CERLUX CENEFAS.xls
23	6e62059e900969b55ce3df9c	c80f8abc132ca847502693ab4596	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\LISTA PRECIOS PORCELANATO.xls
24	74c492c4b681ea822ddbd9fc	391f4b990963a977e68a661c3559	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\LISTA PRECIOS SR. AUGUSTO LLERENA.xls
25	aaf3ea2d86bf8d96d061ba91	29d9e2633d20f1f4a8197bfef0cc	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\ORDEN COMPRA.BALDOSINESxls.xls
26	22deaf98c1177c04bb7bee5	d189328555e2b9a0e0a8de9dc38	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\ORDEN COMPRA.xls
27	6d128481d5a05ad3ae8cfadf	50ebafaa5f811d6e0edf80fc6f4e	\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\Palm 16'06'08.xls

23	adccfbd10cbccbcce0a60b62	d57a7ae367b16a26ecbff7e1e08f \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\PEDIDO DR. GUERRERO.XLS
29	8959646c17ebdc448d1a796(	125d1d8b277fcc8b0c5941b7305c \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\PEPIDOS1.XLS
30	b5292a0c79ed91b026ff059e	29c0407f7b093ae9dc5558e869e9 \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\POLITICAS DE VENTA.xls
31	d44dc73ecfea3c83f0edac0fe	d4cd214ddcde6b676a02f07c2341 \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\PRECIOSAIIJAJUNIO08.XLS
32	18af7c5c53b8822f94cc6d4ff(	445ccd0ed8f5ec8d4ed7e8f6dd8(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\PROFORMAS LOJA CONSTRDAVID REGALADO.xls
33	f68b3c8d339a8e35b992e39(	1230225baca098c317d134043e7e \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\PROFORMAS LOJA CONSTRUCTORES.xls
34	245cb9d9605e3ba5a0700bc4	305b03d5dcaa46609ee89079c40(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\quotation for floor tile.xls
35	af2f96258380619e3d22bb7b	e27670d3cc6252d3fea91b96158a \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERINCOVA [FAT32]\[root]\mis docuemtos\REPARTO UTILIDADES15% 2008.xls
36	bce993c8d07cd8adfff7df35(	b4ef47899f58aea4df316634e58e \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\usuarios.DBF.XLS
37	359d4268d7c5b57014f28030	43f3e2feaf37643410e83bb40e23 \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\$se32.xls
38	d1d8350d9460fa3ce2a2d4c5	ef64b2f630da381fc254792ba4a2(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\$se32.xls
39	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-1-5-21-1482476501-1644491937-682003330-1013\$in32.xls
40	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-1-6-21-2434476501-1644491937-600003330-1213\$utephoto.xls
41	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\$wgkvsq.xls
42	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\$wgkvsq.xls
43	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\$wgkvsq.xls
44	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\$wgkvsq.xls
45	78c9042bbcefd65beaa0d40(	197e347479b9b6b7cde6c46c5db(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\$wgkvsq.xls
46	48eb25a385f94d8bdc6589f4	d6a4edeac576baae0a5a11af9445 \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\configuxls_cuentas.xls
47	15a759878738f87e8c43e40d	f873a17249a0f328a5dc5e5c8464(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\!APABU~1.xls
48	b921dd642625f31040bcbb7(	c51cb7c43a421875f5e255a4a2ee \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\!.xls
49	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\!scaneo.xls
50	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\!orense.xls
51	8284e836196cf856397db316	ea3da2d0e206c3082db767bf619(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\cetk.xls
52	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\!rafico.xls
53	5bb8b4bf77e60400e3130b6(	eacfadaeb7f205cd3bf4a8cec1dc(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\curriculum1.xls
54	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\curriculum.xls
55	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\Peticio a cerimcova.xls
56	d41d8cd98f00b204e980099(	da39a3ee5e6b4b0d3255bfef956(\\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\!RESRE~1.xls
57	017932442ed8859b8e469ee(	7f3bda4192d044a4389a4ce309fb \\.\PHYSICALDRIVE2\Partition 1 [78456MB]\CERIMCOVA [FAT32]\[root]\mis docuemtos\0.0.168.in-addr.xls

Imágenes 3.7 y 3.8- Contenido de todo el archivo "reporte.xls" que contiene todos los archivos borrados filtrados por la extensión ".xls" y que serán analizados para encontrar indicios que permitan obtener evidencias.

3.4 Análisis Forense de la Importadora

Evidentemente la labor de todo perito informático es obtener evidencia relevante, autentificable, verificable, y neutral. Quienes realizamos esta monografía siguiendo con esta labor, analizamos y obtuvimos información contemplada en los puntos 3.2 y 3.3 de este capítulo, basándonos en el marco técnico – teórico descrito en el capítulo 2 (concretamente en el punto 2.5 Análisis forense)

Lo que se procede a realizar en este punto es analizar la imagen obtenida en el punto anterior el 3.3 y utilizaremos las siguientes herramientas:

- Mount Image Pro v2.60: herramienta que permite "montar" imágenes de cualquier extensión.
- PC Inspector File Recovery versión 4.0: herramienta que permite recuperar archivos borrados.

- disco duro externo de marca:”Maxtor” con la serie: 57212120414281DFZXX que se lo conectara en el puerto USB en donde se encuentra la primera imagen almacenada para poderla analizar con las dos herramientas anteriores.

- Una computadora portátil Hewlett Packard modelo Pavilon dv9000 con la serie: CNF6401JZZ, perteneciente al Sr. Andrés Córdova en donde se analizará la información obtenida

Ponemos a consideración la Bitácora de sucesos realizados del Viernes 8 al Sábado 9 de Mayo del 2009.

Paso b1.- Aspectos preliminares del análisis de la información obtenida:

Llegada de los peritos a la “CERIMCOVA” se hizo una reunión con el Gerente para informarle y discutir como, que metodología emplear y que herramientas utilizar para analizar los indicios obtenidos los cuales son objeto de un análisis minucioso.

b1.1 En la computadora portátil Hewlett Packard modelo Pavilon dv9000 con la serie: CNF6401JZZ con la herramienta Mount Image Pro v2.60 se procede a montar la imagen obtenida (“cerincova.dd”) y realizar un profundo análisis.

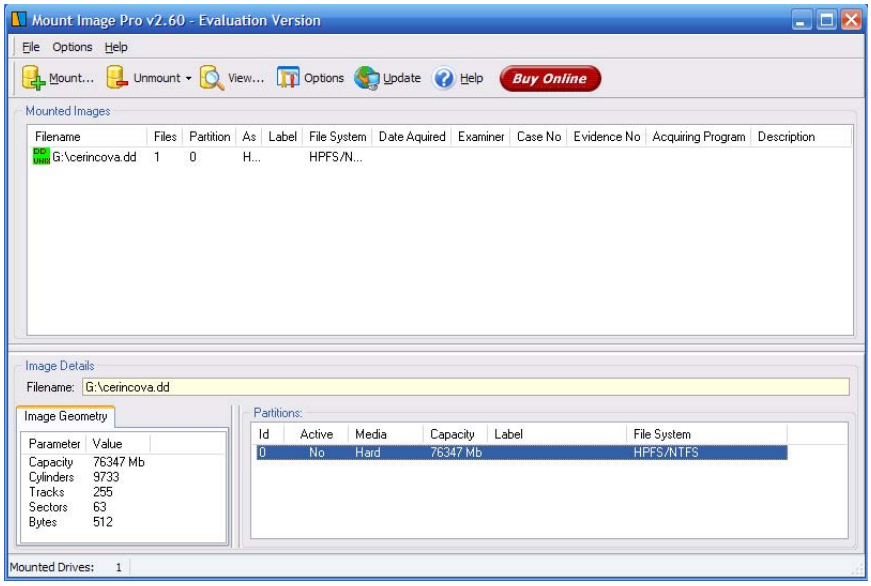


Imagen 3.9- Con el programa Mount Image se monta la imagen para analizarla.

Paso b2.- Adquisición de los archivos borrados con la herramienta PC Inspector File Recovery

En la computadora portátil Hewlett Packard modelo Pavilon dv9000 con la serie: CNF6401JZZ con la herramienta PC Inspector File Recovery versión 4.0 se procede a recuperar todos los archivos borrados de la imagen obtenida en los pasos anteriores.

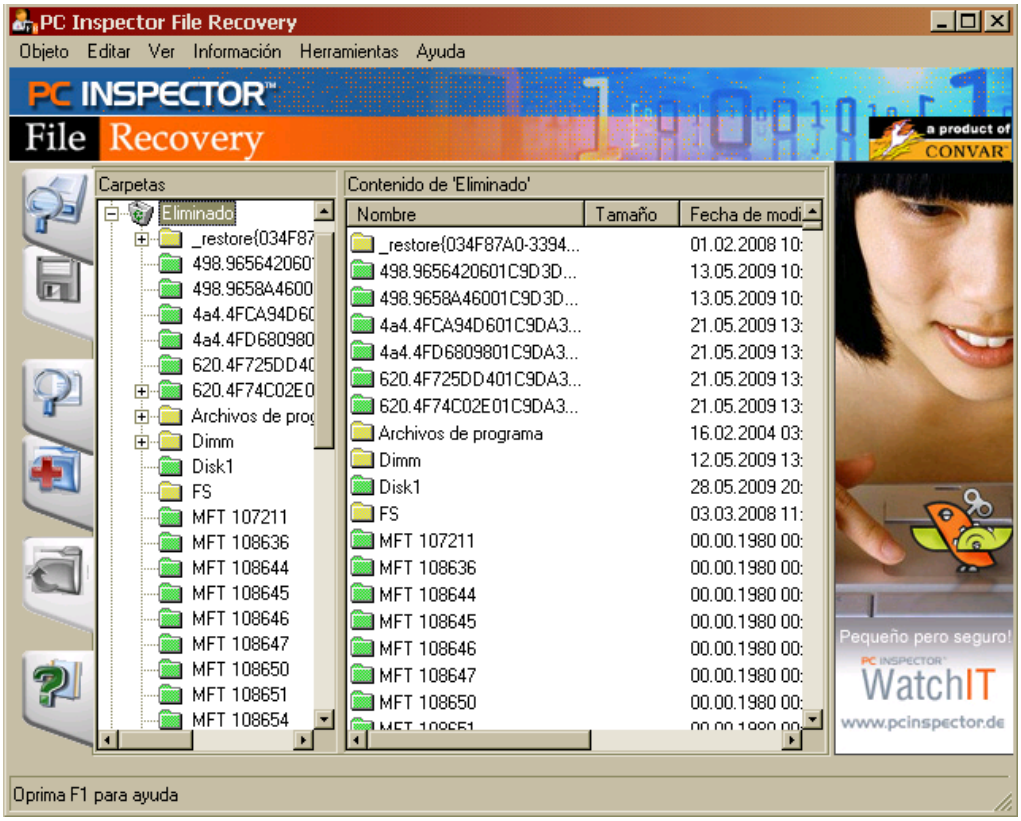


Imagen 3.10- Pc Inspector analiza la imagen extraída.

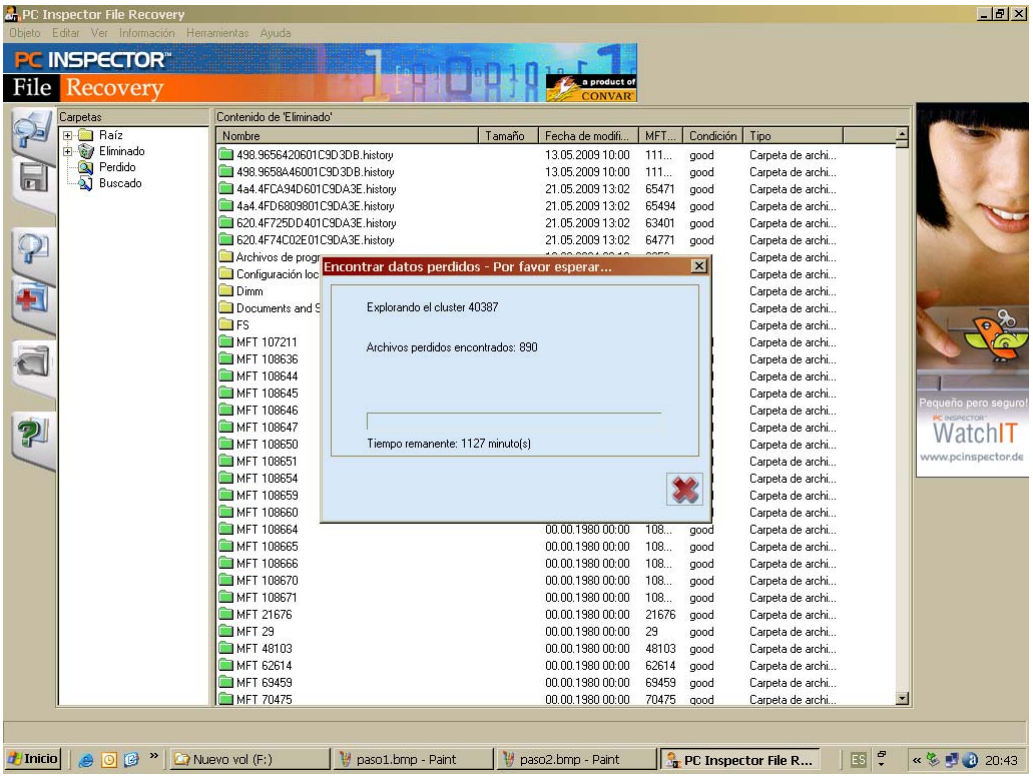


Imagen 3.11- Pc inspector recuperó todos los archivos borrados.

b2.1 - Se procede a filtrar los archivos borrados encontrados con la extensión "*.xls" y guardarlos en una carpeta llamada "archivos" que se encuentra ubicada en la computadora portátil Hewlett Packard modelo Pavilon dv9000 con la serie: CNF6401JZZ, en la dirección "C;\Documents and Settings\Andres Cordova\Desktop\archivos" para encontrar algún indicio que nos conduzca a la evidencia.

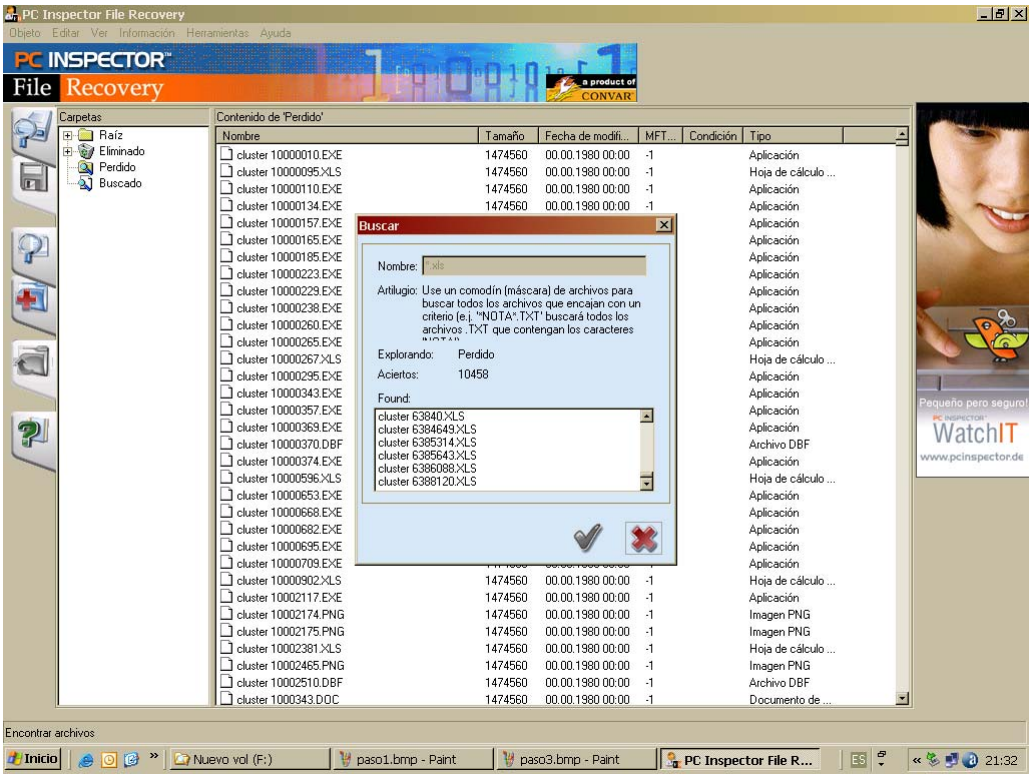


Imagen 3.12- Pc inspector recuperó todos los archivos borrados con la extensión ".xls".

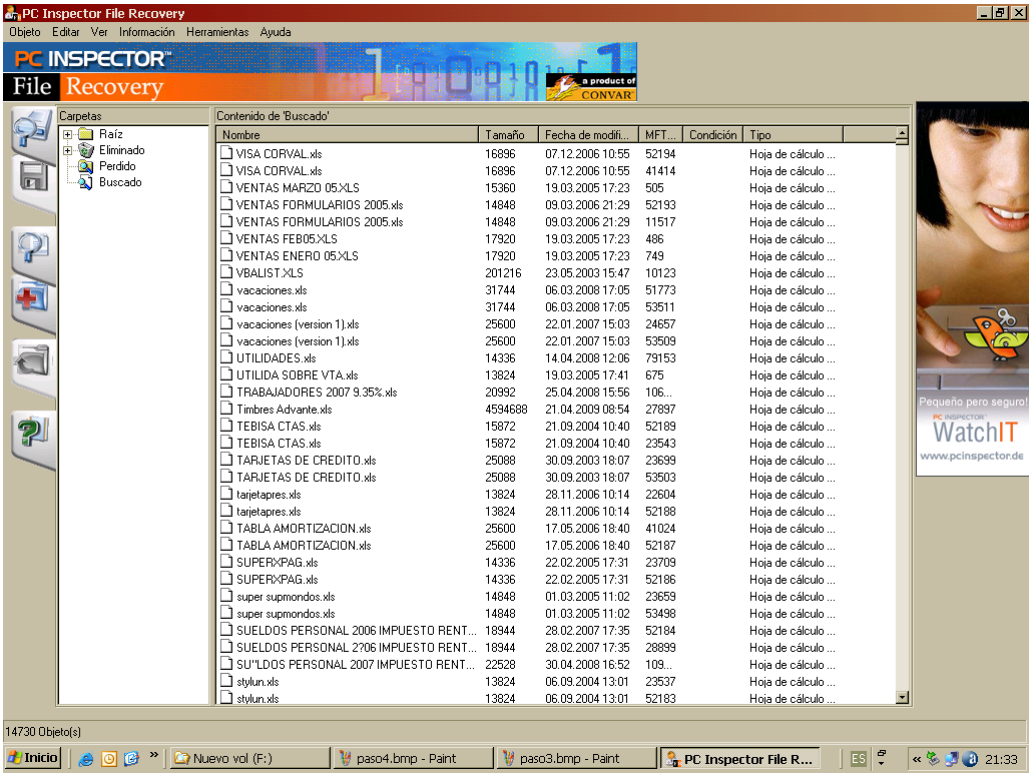


Imagen 3.13- Con Pc inspector se procedió a exportar y recuperar los archivos ".xls".

Paso b3.- Búsqueda de archivos recuperados con la herramienta PC Inspector y filtrar por las fechas en la que pudo haber vulnerabilidades con la privacidad de la información en el sistema.

Se procede a filtrar los archivos borrados recuperados guardados en la carpeta "archivos" con extensión "*.xls" por las fechas comprendidas entre Junio-Septiembre del 2008, donde se obtuvieron 56 archivos y se los analizó uno por uno hasta que se encontró la evidencia.

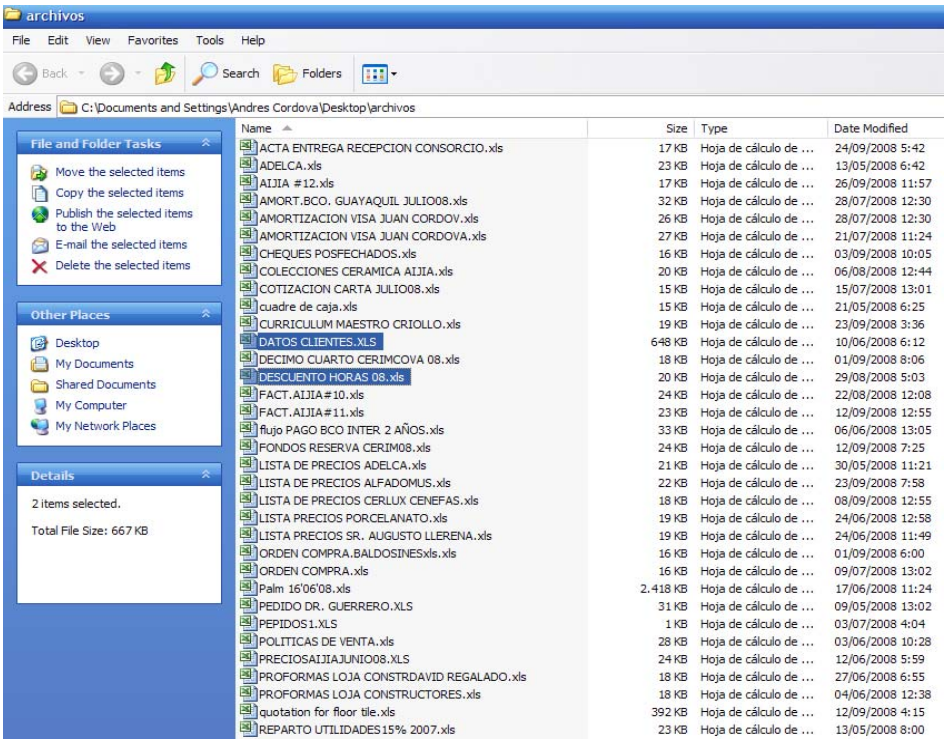


Imagen 3.14- Pc inspector recuperó todos los archivos borrados con la extensión ".xls" y lo filtramos por el rango de fechas Junio – Septiembre 2008.

b3.1- Los archivos: "DATOS CLIENTES.XLS" y "DESCUENTO HORAS 08.XLS" tienen información confidencial de "CERIMCOVA" y su

generación no fue autorizada por ningún Directivo lo que se constituye como evidencia. A continuación se presenta parte de la información de estos archivos:

b3.2- “DATOS CLIENTES.XLS”. fue generado el 10/06/2008 6:12 p.m. y contiene 1180 líneas:

Microsoft Excel - DATOS CLIENTES

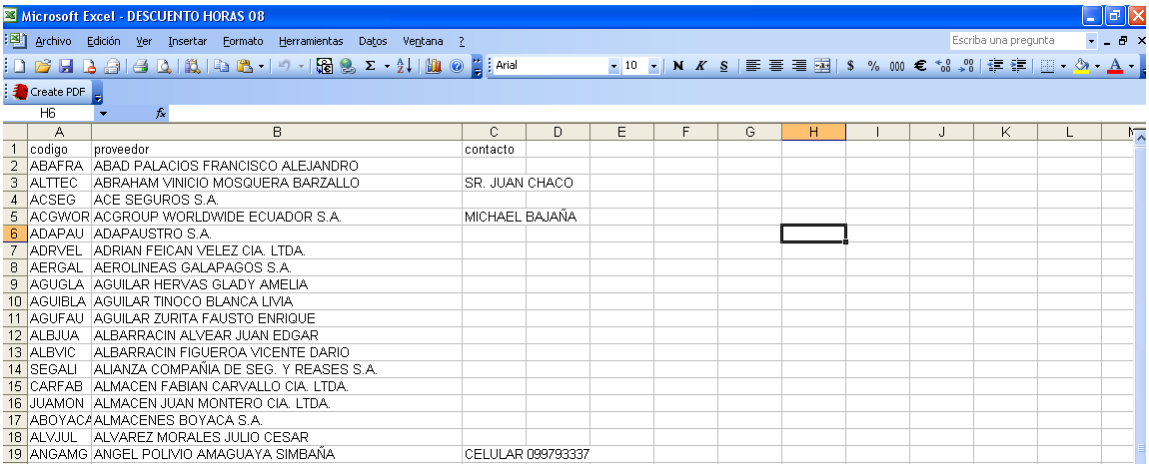
Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

C7 MANUEL MORENO Y MIGUEL DIAS

	A	B	C	D	E	F	G
1	codigo	cliente	direccion	telefono	ciudad	ultimavta	promedio
2	ABCJOS	ABACO JOSE	ELOY ALFARO	2850469	CUENCA		0
3	ABAFRA	ABAD ABRIL FRANKLIN	UNIDAD NACIONAL Y PASEO TRES	817074-840440	CUENCA		0
4	ABAJUA	ABAD GUZMAN JUAN	LUIS CARLOS JARAMILLO Y AV. B.	887813-885982	CUENCA		0
5	ABAPAB	ABAD HERRERA PABLO	MIGUEL ANGEL ESTRELLA 5-31	866197-824742	CUENCA		0
6	ABAINI	ABAD IÑIGUEZ CIA. LTDA.	JOSE PERALTA 1-124 Y CORNELIO	2814666	CUENCA		0
7	ABMAR	ABAD MARIA CARIDAD	MANUEL MORENO Y MIGUEL DIAS	092968593M	CUENCA		0
8	ABAPAT	ABAD PATRICIO DR.	FRANCISCA DAVILA 1-64	2839245	CUENCA		0
9	ABAEST	ABAD SARMIENTO ESTEBAN	DIEGO VELASQUEZ S/N Y DON BO	880491-885611	CUENCA		0
10	ABAFER	ABARCA FERNANDO ARQ.	RICAURTE	2476311	CUENCA		0
11	ABRADR	ABRIL CABRERA ADRIAN	EL BATAN 5-92	817730	CUENCA		0
12	ABRPA	ABRIL PATRICIO ING	BURBANO	094138814	CUENCA		0
13	ACOJUA	ACOSTA VASQUEZ JUAN	AV.REMIGIO CRESPO 1-128	831222	CUENCA		0
14	AGUFRD	AGUILAR AGUILAR FREDY TEODORO	VEGA MUÑOZ 5-51	844120	CUENCA		0
15	AGUNEL	AGUILAR SANCHEZ NELSON	SUCRE 3-12	826125	CUENA		0
16	AGUAUG	AGUILAR VNTIMILLA AUGUSTO	LARGA 9-60	880362-839297	CUENCA		0
17	AGUPAT	AGUIRRE PATRICIO	ABERLARDO J ANDRADE	2857377	CUENCA		0
18	ALBVIC	ALBARRACIN FIGUEROA VICENTE	GONZALEZ SUAREZ 16-38 Y GENEF	2806053	CUENCA		0
19	ALBMARIE	ALBARRACIN MARIBEL	ALEXANDER FLEMEN YABELARDO	4081591	CUENCA		0
20	JUAALB	ALBORNOS JUAN CARLOS	MANUEL VEGA 9-97 Y GRAN COLO	835143	CUENCA		0
21	ALBMAR	ALBUJA MARCELO	CALLA 6TA.#207 Y AV. 3ERA. (URDI	2388783	GUAYAQUIL		0
22	ALEVIC	ALEMAN VICTOR ARQ.	DOS CUADRAS ANTES DE LA IGLE	2892818	CUENCA		0
23	ALFRIO	ALFREDO RIOS VEGA ARQ.	PASEO 3 DE NOVIEMBRE Y ESCAL	2839827-840061	CUENCA		0
24	ALIGLA	ALIGLA S.A.	GIL RAMIREZ DAVALOS #3-86	2871952	CUENCA		0
25	ALMFRA	ALMACHE FRANCISCO	AV. LOJA 2-20 Y LORENZO PIEDRA	2815687	CUENCA		0
26	ALTEDG	ALTAMIRANO JARA EDGAR	HUAYNA CAPAC 4-30	825802	CUENCA		0
27	ALTIVA	ALTAMIRANO JARA IVAN ARQ-	AV. J. ANDRADE Y DEL CHOFER	408367	CUENCA		0
28	ALTJED	ALTAMIRANO JEANNETT DE B.	AV. SOLANO Y NICANOR AGUILAR	2816794-2891826	CUENCA		0
29	ALTJEA	ALTAMIRANO LEON JEANNETH	DAVID DIAZ 1-52	891081-816794	CUENCA		0
30	ALVMAR	ALVARADO ARGUDO MARCO	MANUEL ORMAZA 3-19	816227	CUENCA		0
31	ALVCES	ALVARADO CESAR SR.	JAIME ROLDOS Y L CORREA	2255207	GUALACEO		0
32	ALVDIE	ALVARADO CORRAL DIEGO	TOMAS ORDOÑEZ 9-18	829251-2814272	CUENCA		0
33	ALVEDU	ALVARADO EDUARDO	REMIGIO CRESPO 1308	2818284	CUENCA		0
34	ALVHER	ALVARADO HERNAN OSWALDO	FRENTE COLEGIO TURI	821176	CUENCA		0

Imagen 3.15- Contenido de DATOS CLIENTES.XLS que contiene los datos de los clientes de CERIMCOVA.

b3.3- “DESCUENTO HORAS 08.XLS” fue generado el 29/08/2008 5:03 p.m y contiene 287 líneas.



Microsoft Excel - DESCUENTO HORAS 08

	A	B	C
1	codigo	proveedor	contacto
2	ABAFRA	ABAD PALACIOS FRANCISCO ALEJANDRO	
3	ALTTEC	ABRAHAM VINICIO MOSQUERA BARZALLO	SR. JUAN CHACO
4	ACSEG	ACE SEGUROS S.A.	
5	ACGWOR	ACGROUP WORLDWIDE ECUADOR S.A.	MICHAEL BAJAÑA
6	ADAPAU	ADAPAUSTRO S.A.	
7	ADRVEL	ADRIAN FEICAN VELEZ CIA. LTDA.	
8	AERGAL	AEROLINEAS GALAPAGOS S.A.	
9	AGUGLA	AGUILAR HERVAS GLADY AMELIA	
10	AGUIBLA	AGUILAR TINOCO BLANCA LIVIA	
11	AGUFAU	AGUILAR ZURITA FAUSTO ENRIQUE	
12	ALBJUA	ALBARRACIN ALVEAR JUAN EDGAR	
13	ALBVIC	ALBARRACIN FIGUEROA VICENTE DARIO	
14	SEGALI	ALIANZA COMPAÑIA DE SEG. Y REASES S.A.	
15	CARFAB	ALMACEN FABIAN CARVALLO CIA. LTDA.	
16	JUAMON	ALMACEN JUAN MONTERO CIA. LTDA.	
17	ABOYACA	ALMACENES BOYACA S.A.	
18	ALVJUL	ALVAREZ MORALES JULIO CESAR	
19	ANGAMG	ANGEL POLIVIO AMAGUAYA SIMBAÑA	CELULAR 099793337

Imagen 3.16- Contenido de DESCUENTO HORAS 08 que contiene la información de los proveedores de CERIMCOVA.

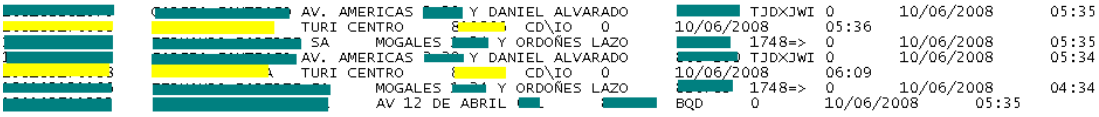
Paso b4.- Búsqueda de los usuarios que estuvieron logeados en la Base de Datos de acuerdo a las fechas en las que se originó la evidencia

Procedemos a verificar los accesos a la Base de Datos en las fechas que se generaron los 2 archivos sospechosos encontrados.

b4.1- Para comprobar el acceso al sistema en la fecha que se generó “DATOS CLIENTES.XLS” a continuación ponemos el log de acceso:

Usuario Secretaria 1: Amarillo

Otros usuarios: Cardenillo



```
[redacted]  [redacted] AV. AMERICAS [redacted] Y DANIEL ALVARADO  [redacted] TJDXJWI 0  10/06/2008  05:35
[redacted]  [redacted] TURI CENTRO  8[redacted] CD\IO  0  10/06/2008  05:36
[redacted]  [redacted] SA  MOGALES [redacted] Y ORDOÑES LAZO  [redacted] 1748=>  0  10/06/2008  05:35
[redacted]  [redacted] AV. AMERICAS [redacted] Y DANIEL ALVARADO  [redacted] TJDXJWI 0  10/06/2008  05:34
[redacted]  [redacted] TURI CENTRO  8[redacted] CD\IO  0  10/06/2008  06:09
[redacted]  [redacted] MOGALES [redacted] Y ORDOÑES LAZO  [redacted] 1748=>  0  10/06/2008  04:34
[redacted]  [redacted] AV 12 DE ABRIL [redacted]  [redacted] BQD  0  10/06/2008  05:35
```

Imagen 3.17- log de los usuarios el 10/06/2008.

b4.2- Para comprobar el acceso al sistema en la fecha que se generó “DESCUENTO HORAS 08.XLS” a continuación ponemos el log de acceso:

Usuario Secretaria 1: Amarillo

Otros usuarios: Cardenillo

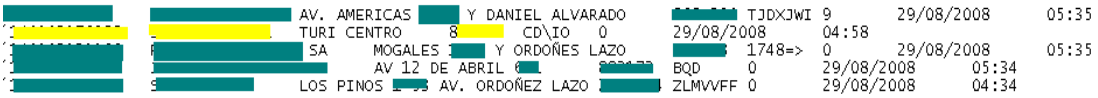


Imagen 3.18- log de los usuarios el 29/08/2008

Utilizando una metodología técnica especializada y en conformidad con la ley, siguiendo cada momento los principios fundamentales de la información forense, documentado paso a paso el proceso investigativo se procede a comprobar si es que el sistema permite generar los archivos encontrados como evidencia y verificar quien los genera.

Para realizar esto se solicita al jefe del Departamento de Sistemas la creación de una perfil llamado "AUDITOR" con los mismos privilegios y permisos del usuario "*Secretaria 1*" (anexo 13), con el objeto de comparar la evidencia obtenida generada por el usuario "*Secretaria 1*".

Ponemos a consideración los sucesos realizados el 15 de Mayo del 2009.

I- Ingreso al Sistema de Facturación con el perfil "AUDITOR"

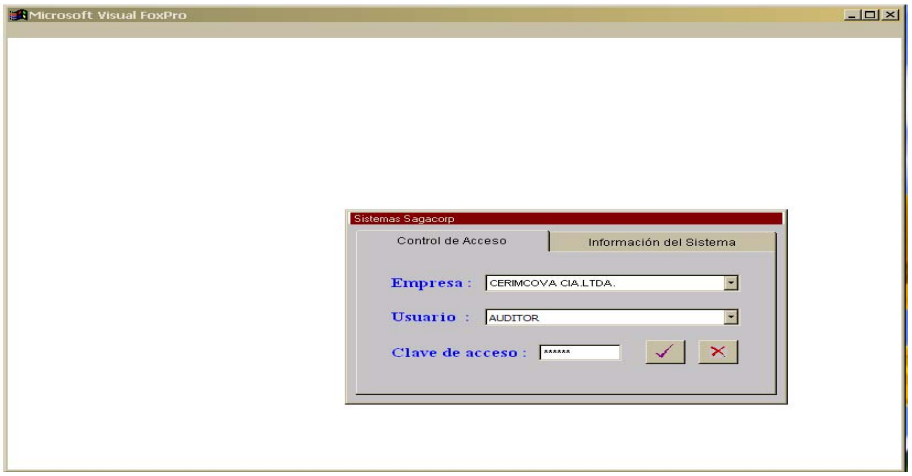


Imagen 3.19- Ingreso al sistema de facturación por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

II- Ingreso al Menú Principal

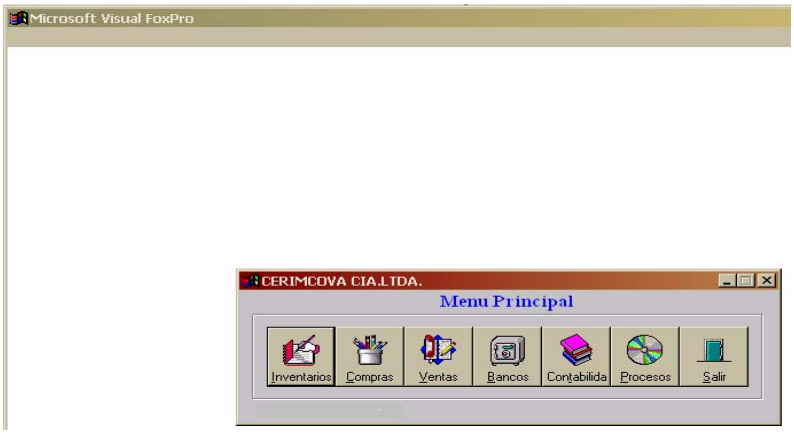


Imagen 3.20- Ingreso al menú principal por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

III- **Ingreso al menú de Compras-Proveedores**:

Imagen 3.21- Ingreso al menú de Compras por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

IV- Ingreso a la opción Proveedor y detalle del proveedor:

Imagen 3.22- Ingreso al detalle de proveedores por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

V- Ingreso a la opción imprimir proveedores y guardar en un archivo Excel:

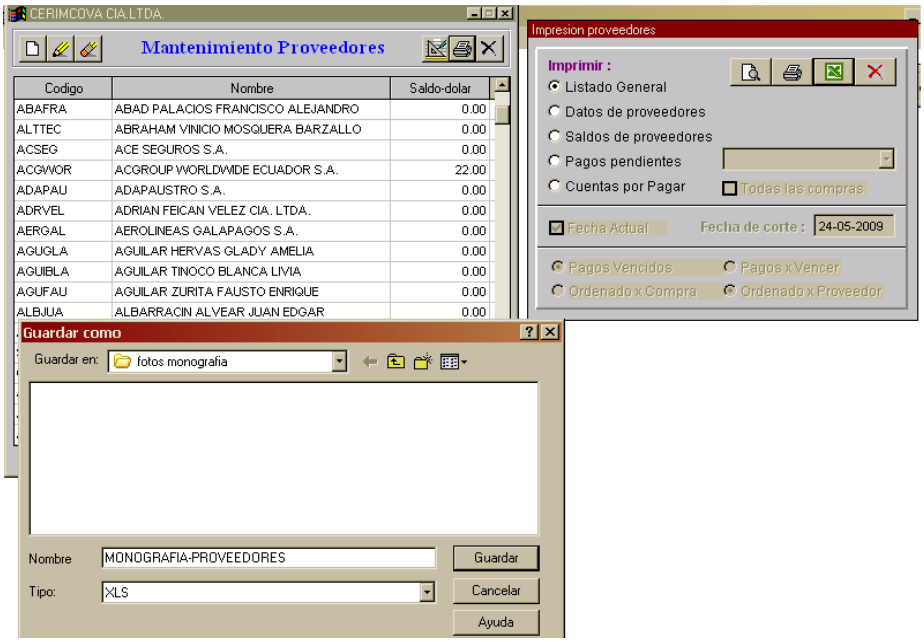


Imagen 3.22- generar archivos de proveedores en excel por los peritos.

Se obtiene un archivo llamado MONOGRAFIA-PROVEEDORES que contiene 299 provedores:

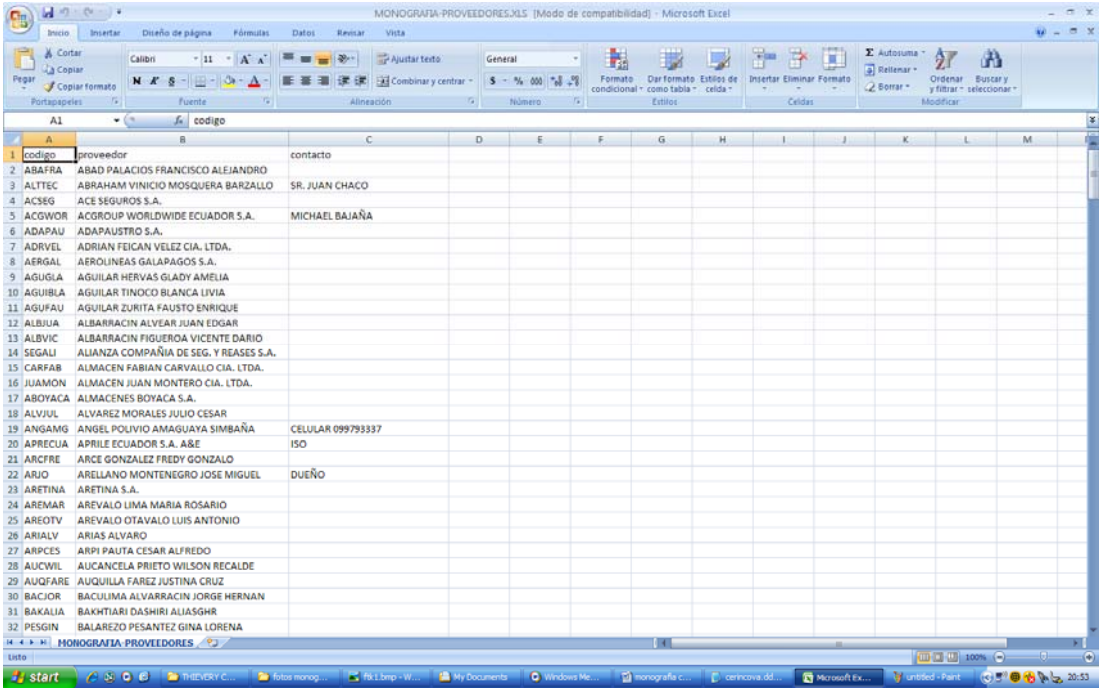


Imagen 3.23- archivo de proveedores obtenido por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

VI- Ingreso al menú de Ventas-Clientes:

Imagen 3.24- Ingreso al menú de Clientes por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

VII- Ingreso a la opción de Clientes y detalles de clientes:

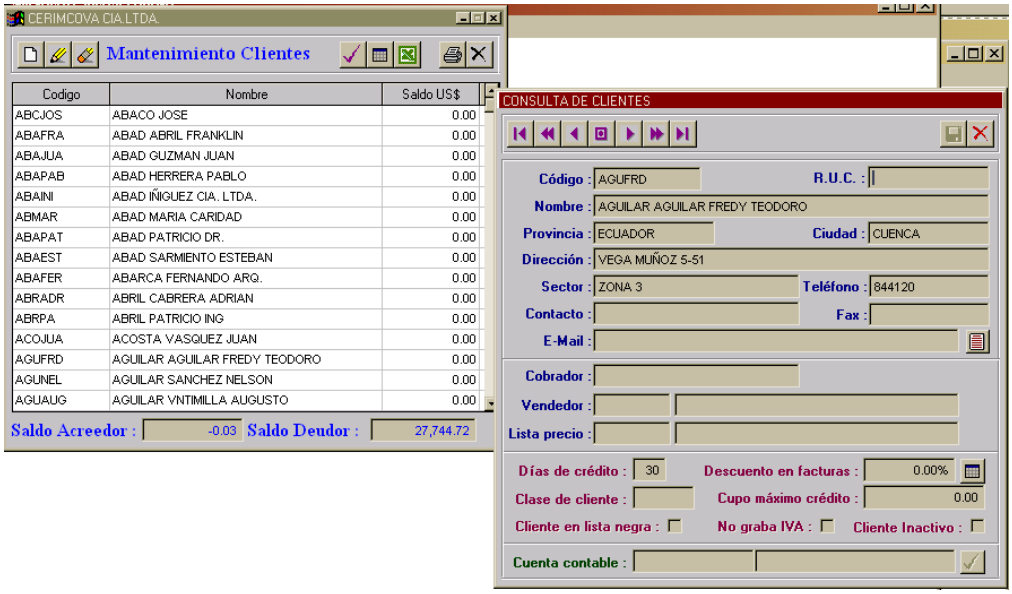


Imagen 3.25- Ingreso detalle de Clientes por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

VIII- Ingreso a la opción Imprimir clientes y guardar en un archivo Excel:

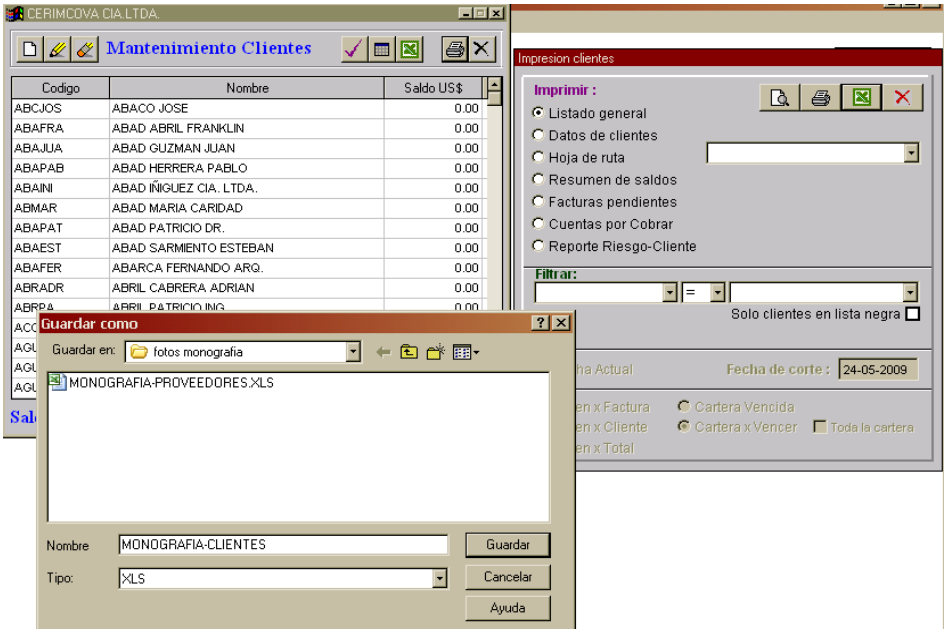


Imagen 3.26- Generar un archivo de Clientes por los peritos

Se obtiene un archivo llamado MONOGRAFIA-CLIENTES que contiene 1197 clientes:

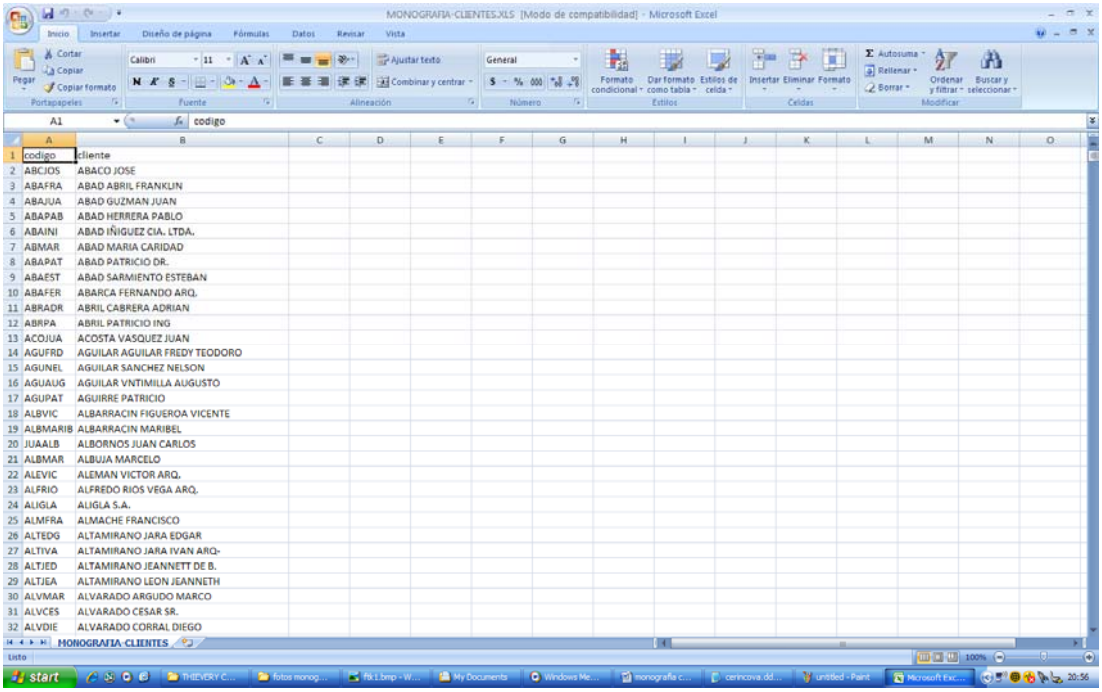


Imagen 3.27- archivo de Clientes obtenido por los peritos

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

IX- Verificamos el log de la Base de Datos:

```
L6010460682     AUDITOR     CERIMCOVA     832-484     TJDXJWI     9     15/05/2009     22:10
```

Imagen 3.28- log que nos indica quien estuvo logueado en la base de datos del sistema de facturación de CERIMCOVA

Responsables: Andrés Córdova.

Supervisores: Esteban Piedra, Moises Leser.

El sistema de facturación de la Importadora “CORVAL Cía. Ltda.” en la permitió con el usuario “AUDITOR” obtener dos archivos: “MONOGRAFIA-PROVEEDORES.XLS” con 299 proveedores y “MONOGRAFIA-CLIENTES.XLS”

con 1197 clientes, mientras que los archivos generados por el usuario "*Secretaria 1*" fueron: "DATOS CLIENTES.XLS" con 1180 clientes y "DESCUENTO HORAS 08.XLS" con 287 proveedores ; lo cual nos deja entrever que el usuario "AUDITOR" que tiene los mismos permisos o privilegios que tenía el usuario "*Secretaria 1*" pudo generar información tanto de Clientes como de Proveedores.

Con el procedimiento descrito confirmamos que de la computadora clon marca "Mega Clon" se obtuvo:

- A la hora: 6:12 p.m., con fecha: 10/06/2008 ingresaron al sistema de facturación de la Importadora "CORVAL Cía. Ltda." y se obtuvo el archivo: "DATOS CLIENTES.XLS" que tenia información del detalle de clientes para luego ser borrado de la computadora.

- A la hora: 5:03 p.m., con fecha: 29/08/2008 ingresaron al sistema de facturación de la Importadora "CORVAL Cía. Ltda." y se obtuvo el archivo: "DESCUENTO HORAS 08.XLS" que tenía información del detalle de proveedores para luego ser borrado de la computadora.

Esta computadora estaba a cargo de "*Secretaria 1*" de acuerdo al Acta entrega-recepción (anexo 2) firmada con fecha: 10/01/2006.

Esta información constituye la evidencia necesaria para que los Directivos tomen las acciones que consideren pertinentes.

3.5 Presentación Judicial

Informe Pericial realizado por los estudiante de la Universidad del Azuay escuela de Ingeniería de sistemas previo a la obtención del Título que suscribe en relación con el Oficio enviado al Gerente General de la Empresa CERIMCOVA CIA. LTDA. Sr. Moisés Leser, seguido en contra de la Señor(a) secretaria1.

Sr. Andres Esteban Cordova Valverde

CI: 0104260682

Sr. Paul Esteban Piedra Dominguez

CI: 0103884656

Los peritos que suscriben Andrés Córdova, Esteban Piedra declaran decir la verdad y que ha elaborado el presente informe en forma objetiva y teniendo en consideración, por tanto, todos los elementos que influyen en el objeto estudiado.

Contenido

OBJETIVO

Conforme el Acta de Posesión del día 14 de Enero del 2009, en virtud del escrito CARTA dirigida a Importadora CERIMCOVA de proceso (anexo5), se deberá proceder a establecer lo siguiente:

A verificar si es dio la posible fuga de información y determinar en donde se realizo el hecho y además indicar la forma que se pudo realizar y demostrar las posibles falencias en el sistema, controles y las seguridades.

METODOLOGIA EMPLEADA

Para la realización del presente peritaje se ha utilizado una metodología técnica especializada y de conformidad a la ley, siguiendo cada momento los principios fundamentales de la información forense, documentando totalmente y a fondo el proceso investigativo, utilizado herramientas hardware adecuadas y herramientas software forenses especializadas.

Para la consecución del objeto de este peritaje se utilizaron las aplicaciones: Hélix Ver. 1.8, Mount Image Pro Ver.2.60 , y PC Inspector File Recovery Ver.4.0 , para el análisis se utilizaron las aplicaciones: Microsoft Excel 2007 y la aplicación de Búsqueda de Windows XP.

DESCRIPCION DEL PROCESO

El proceso se compone de dos partes, la primera parte se centra en verificar respecto al ingreso de la información a la aplicación de Sistema de Facturación en la base de datos de Visual Fox Pro para consultar información relativa a clientes, proveedores y artículos por el año 2008, y la segunda parte se centra en la verificación acerca de la existencia, borrado o destrucción de archivos tipo Excel relacionados con la consulta.

PROCESO DE LA OBTENCION DE LA PRUEBA

El día 1 de Mayo del 2009 a las 9H00 Pm en la ciudad de Cuenca en la Oficinas de la Importadora CERIMCOVA CIA LTDA ubicado en el edificio CORVAL en las calles Ave. 12 de Abril y Unidad Nacional, en el área de Ventas como parte del peritaje y bajo la presencia del Sr. Moises Leser con CI 0923277602 se procedió a identificar el computador que se encuentra asignado a la señora secretaria1 el mismo que se encuentra identificado con el número de serie 6Y33KN9Z-5006.

Se solicito la presencia del Sr. Moises Leser, con CI 0923277602 como observador del proceso (anexo6).

A las 21 horas 11 minutos 40 segundos del día 1 de Mayo del 2009 se procedió a obtener una imagen lógica del disco duro del computador mencionado para lo cual se utilizo la aplicación software FTK contenida en la herramienta forense HELIX, proceso que culmino a las 21 horas 1 minuto 00 segundos del día 2 de Mayo del 2009, una vez obtenida la imagen se verifico su originalidad y autenticidad utilizando el algoritmo MD5, obteniendo el siguiente hash: fd58aaaa40e3c88e8bb739d5fab8b53f (anexo7).

A las 21 horas 20 minutos 35 segundos del día 2 de Mayo del 2009 se procedió a obtener una imagen lógica del disco duro del computador mencionado para lo cual se utilizo la aplicación software FTK contenida en la herramienta forense HELIX, proceso que culmino a las 21 horas 40 minutos 37 segundos del día 3 de Mayo del 2009, una vez obtenida la imagen se verifico su originalidad y autenticidad

utilizando el algoritmo MD5, obteniendo el siguiente hash: fd58aaaa40e3c88e8bb739d5fab8b53f (anexo8).

Para constancia lo mencionado, la actividad realizada durante este día se la registro en un Acta Pericial (anexo9), suscrita por el perito, por los Señores Andrés Córdova CI: 0104260682, Esteban Piedra CI: 0103884656 y por Sr. Moises Leser con CI 0923277602.

El día 3 de Mayo del 2009 a las 21:50 p.m. en la ciudad de Cuenca en las oficinas de CERIMCOVA ubicado en las calles Ave. 12 de Abril y Unidad Nacional, como parte del peritaje se procede a solicitar al Ing. Santiago García que menciona es el encargado y administrador del aplicativo Sistema de Facturación muestre el log de acceso y las consultas realizadas en la aplicación por la secretaria1 durante el último año 2008 (anexo10), y muestre el proceso de generación de reportes del accesos a la aplicación Clientes, Proveedores y Artículos.

De este proceso se pudo obtener 2 archivo txt:

Usuarios.dbf100608.txt(anexo11)
Usuarios.dbf290808.txt(anexo12)

VERIFICACION DE EXISTENCIA, BORRADO O DESTRUCCION DE ARCHIVOS TIPO XLS

Se inicio el 1 de Mayo del 2009 a las 23 horas 5 minutos, se procedió a identificar el computador que se encuentra asignado a la secretaria1 el mismo que muestra el número de serie 6Y33KN9Z-5006.

Se solicito al señor Moises Leser proceda a prender la computadora e ingresar a la misma con el usuario administrador, una vez ingresado en la computadora, se procedió a obtener información referente a actividades realizadas en el computador en la fecha viernes 1 de Mayo del 2009.

Posteriormente se reviso el perfil de usuario y confirmación de las propiedades del mismo (imagen3.1).

Se procedió a buscar archivos EXCEL (.xls) que puedan tener relación con la información desplegada en los reportes de consulta consolidada del contribuyente, específicamente se busco lo siguiente:

- Archivos de tipo .xls modificados entre el junio 2008 y Septiembre 2008. Se obtuvieron 56 archivos (imagen 3.14).

Con la finalidad de analizar el objeto de la pericia, encaminada a la verificación de borrado o destrucción de archivos tipo XLS, realizo el proceso de recuperación de

información y se analizo el registro de aplicaciones y lista de programas instalados para buscar la existencia de algún tipo de software destructor de información.

El proceso realizado durante este día se lo registro en una Acta Pericial (anexo9), y para constancia de lo actuado suscribieron la mencionada acta, junto a los peritos, Ing. Santiago García con CI: 0103864028 e Sr. Moises Leser con CI 0923277602 como observadores y testigos del proceso.

PROCESO DE ESTUDIO DE LA PRUEBAS OBTENIDAS

Para analizar las imágenes obtenidas se utilizo el software Mount Image Pro Ver. 2. Y Microsoft Excel.

ANALISIS DE LA PRUEBA PERICIAL

El dictamen pericial se presenta en forma conclusiones e indicios.
Las conclusiones son aseveraciones inequívocas que no están sujetas a validación o refutación, por encontrarse apoyadas en principios doctrinales y técnicos irrefutables.

Los Indicios son los que quedan supeditados a otros trabajos de peritaje o validación mediante presentación de pruebas de partes que apoyen o descarten los mismos. No generan una conclusión por sí mismo, solo abren posibles líneas de investigación.

CONCLUSIONES

Aplicación

- De reporte generado (anexo11-12) se pudo observar que el usuario secretaria1 durante el año 2008 realizo varias consultas a información de clientes, proveedores y artículos, todas estas consultas realizadas el 10 de Junio del 2008 a las 6h11 pm y 29 de agosto del 2008 a las 5h01 pm , de las cuales, en estas consultas se visualizo y exporto información fuera de horas laborables.

Verificación de la información en formato Excel.

- En la computadora de uso de la secretaria1 que muestra el numero de serie 6Y33KN9Z-5006, marca Mega Clon, Modelo Clon, se pudo observar la existencia de archivos relacionados con la pericia (anexo2).
- Se pudo observar la existencia de archivos creados entre mayo y el septiembre.
- De los 56 archivos de tipo .xls que se encuentran en el computador se uso filtro desde la fecha mayo y junio del 2008, lo cual aparentemente indica que todos estos archivos fueron copiados en esa fecha en el computador mencionado.
- Se pudo observar que el usuario secretaria1 genero archivos de consulta de proveedores y clientes en fechas antes de salir y en horas fuera de horas laborables.

- Del proceso de recuperación de información se encontraron 14730 archivos eliminados, algunos relacionado con el objeto del presente peritaje, de lo cual se concluye que se abría eliminado archivos de tipo .xls (Excel).

INDICIOS:

Se presentan indicios en el estudio pericial de la evidencia.

OBSERVACIONES FINALES

Dentro de las funciones para las cuales se me ha posesionado, se puede precisar las siguientes observaciones:

- Se intento en todo momento cumplir con la labor pericial dentro de un marco de respeto y legalidad, explicando a todas las partes los alcances y limitaciones de la tarea pericial.
- Se realizaron las diligencias escritas que se consideraron oportunas y pertinentes, con objeto de certificar la tarea realizada y evitar posteriores mal entendidos.

ANEXOS Y SUSTENTO LEGAL

El presente informe cumple con los Art. 98 y 110 del código de procedimiento penal 2000 en lo que respecta a la prueba material y Art.257 del código de procedimiento civil. La respectiva Acta de Posesión de fecha 14 de enero del 2009 se encuentra incorporada en el respectivo proceso.

Cumpliendo con el Art. 98 Art.257 del antes mencionado cuerpo, se adjunta al presente las pruebas obtenidas, consistentes :

Conclusión Capítulo III:

Después del profundo análisis forense descrito en este capítulo y gracias a las facilidades que se nos ha otorgado por parte de los Directivos de “CERIMCOVA”, se ha obtenido evidencia necesaria que demuestra que del usuario “Secretaria 1” se generó los archivos: “DATOS CLIENTES.XLS” generado el 10/06/2008 6:12 p.m. y “DESCUENTO HORAS 08.XLS” generado el 29/08/2008 5:03 p.m., y que contenían información, el primero de clientes y el segundo de proveedores que son de carácter privado y no tenían autorización alguna por ningún directivo para ser creados y posteriormente ser borrados.

En la computadora que se originó los archivos mencionados, estaba a cargo de “Secretaria 1” de acuerdo al Acta entrega-recepción (ANEXO 2) firmada con fecha: 10/01/2006.

Esperamos que las pruebas presentadas puedan servir a los Directivos para que con gran seguridad y certeza tomen acciones correctas y acertadas para que a la Importadora no se la perjudique en una forma económica, operativa y humana.

Capítulo IV

4.1 Conclusión

Podemos decir que la "Importadora CERIMCOVA Cía. Ltda." es una empresa joven integrada por familiares que ha logrado confiabilidad y prestigio a través de los años que lleva en el mercado debido a la exclusividad en sus productos y clientes.

Competitivamente hablando esta opera en un entorno relativamente estable, el sector de la comercialización es sumamente competitivo, entre los principales competidores esta Importadora Vega, Boyaca, etc., los cuales aprovechan permanentemente todas las oportunidades a su alcance para tomar la delantera. Sin embargo, CERIMCOVA se ha mantenido debido al servicio que brinda a sus clientes.

Revisando y analizando todo lo investigado en el capítulo 1 podemos llegar a la conclusión que se determino como vulnerabilidad y objeto de estudio los movimientos o acciones del usuario "Secretaria 1" concretamente una fuga de información privada de "CERIMCOVA Cía. Ltda." Indicando que es la más factible para realizar estas acciones ya que tenia accesos a la información de Artículos, Proveedores y Clientes, evidenciándose una falta total de normas de Control Interno en la empresa que es objeto de nuestra auditoria.

Esta información pudo haber sido generada en un archivo tipo Excel y después haber sido utilizada con fines perjudiciales para "CERIMCOVA" lo que se constituiría como la respuesta esperada a las sospechas de los Directivos de la Importadora.

Además podemos concluir que se tienen muchos métodos para encontrar o demostrar que se ha cometido fraude o se intento cometer, mediante el análisis y obteniendo las pruebas periciales por medio de la evidencia, contando con herramientas adecuadas que permiten obtener las mismas de forma segura y que los datos no se modifiquen ya que es de suma importancia mantener la información intacta siempre y cuando se sigan las normas establecidas para realizar el análisis forense y para presentar un documento de informe lo mas claro y entendible posible para demostrar la culpabilidad o inocencia de acusado ante el juzgado siempre manteniendo distancia tanto con los implicados y mantener discreción y lo más importante que se tenga todo detallado en bitácoras de lo que se ha hecho y con testigos.

Después del profundo análisis forense descrito en el capítulo III y gracias a las facilidades que se nos ha otorgado por parte de los Directivos de "CERIMCOVA", se ha obtenido evidencia necesaria que demuestra que del usuario "Secretaria 1" se generó los archivos: "DATOS CLIENTES.XLS" generado el 10/06/2008 6:12 p.m. y "DESCUENTO HORAS 08.XLS" generado el 29/08/2008 5:03 p.m., y que contenían información, el primero de clientes y el segundo de proveedores que son de carácter privado y no tenían autorización alguna por ningún directivo para ser creados y posteriormente ser borrados.

En la computadora que se originó los archivos mencionados, estaba a cargo de “Secretaria 1” de acuerdo al Acta entrega-recepción (ANEXO 2) firmada con fecha: 10/01/2006.

Esperamos que las pruebas presentadas puedan servir a los Directivos para que con gran seguridad y certeza tomen acciones correctas y acertadas para que a la Importadora no se la perjudique en una forma económica, operativa y humana

4.2 Recomendación

Después del exhaustivo análisis realizado a “CERIMCOVA” y que se pudo dar una posible fuga de información, la seguridad y confidencialidad de la información en el sistema de facturación requieren, por lo tanto, que se adopten estrictas norma para el proceso de seguridad de los datos agregando un modulo de registro de auditoría con controles de seguridad y con log’s y/o un control extra en el sistemas facturación elaborado en Visual Fox Pro para almacenar información automáticamente cuando ocurre un evento y esta información debe de estar altamente protegida del sistema convirtiéndose así en un mecanismo importante de detección de lo que realizan los usuarios a diario a diferencia de que exista un log o registro interno de la base de datos.

También es necesario que se revisen los perfiles de los usuarios del las funciones que realizan para determinar los permisos necesario cuyas funciones, por su naturaleza, justifiquen tener acceso al sistema mediante los mismos.

Es necesario que a los empleados se les otorgue herramientas necesaria y que no tengan que disponer ellos por sus propios medios, como dispositivo magnéticos o otros equipos que permitan guardar información propia de la empresa, y así evitar y poder verificar que los dispositivos entregados estén dentro de la empresa y no sean llevados por el empleado.