



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES CUAUTILÁN

**“MÉTODO PARA LA RECUPERACIÓN DE INFORMACIÓN EN
DISCOS DUROS ELECTROMECÁNICOS MEDIANTE EL
SOFTWARE: “FERCUVILL V5.0”**

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO ELECTRICISTA

PRESENTA:

FERNANDO CUEVAS VILLALOBOS

ASESOR: ING. JAVIER HERNÁNDEZ VEGA

CUAUTILÁN IZCALLI, ESTADO DE MÉXICO, 2016



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

**FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
UNIDAD DE ADMINISTRACIÓN ESCOLAR
DEPARTAMENTO DE EXÁMENES PROFESIONALES**

U. N. A. M.
FACULTAD DE ESTUDIOS
SUPERIORES-CUAUTITLÁN

ASUNTO: VOTO APROBATORIO



**M. en C. JORGE ALFREDO CUÉLLAR ORDAZ
DIRECTOR DE LA FES CUAUTITLÁN
PRESENTE**

**ATN: M. en A. ISMAEL HERNÁNDEZ MAURICIO
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán.**

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos **La Tesis:**

**“MÉTODO PARA LA RECUPERACIÓN DE INFORMACIÓN EN DISCOS DUROS ELECTROMECÁNICOS
MEDIANTE EL SOFTWARE: “FERCUVILL V5.0”**

Que presenta el pasante: **FERNANDO CUEVAS VILLALOBOS**

Con número de cuenta: **41005154-4** para obtener el Título de: **Ingeniero Mecánico Electricista**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE

“POR MI RAZA HABLARA EL ESPÍRITU”

Cuautitlán Izcalli, Méx. a 13 de mayo de 2016.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Ing. Javier Hernández Vega	
VOCAL	Ing. Oscar Cervantes Torres	
SECRETARIO	Ing. Leonardo Sergio Lara Flores	
1er SUPLENTE	Ing. Luis Raúl Flores Coronel	
2do SUPLENTE	Ing. Gilberto Chavarria Ortiz	

NOTA: Los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional (art. 127).

En caso de que algún miembro del jurado no pueda asistir al examen profesional deberá dar aviso por anticipado al departamento.

(Art 127 REP)

HHA/Vc

ÍNDICE

INTRODUCCIÓN	1
OBJETIVOS	3
OBJETIVO GENERAL	3
OBJETIVOS PARTICULARES	3
CAPÍTULO 1. EL DISCO DURO ELECTROMECAÁNICO	4
1.1 RESEÑAS HISTÓRICAS	4
1.2 DEFINICIÓN DEL DISCO DURO ELECTROMECAÁNICO	10
1.3 ESTRUCTURAS	11
1.3.1 ESTRUCTURA MECÁNICA	12
1.3.2 ESTRUCTURA LÓGICA	43
CONCLUSIONES PARCIALES	64
CAPÍTULO 2. FALLOS EN LAS ESTRUCTURAS	65
2.1 CORRUPCIONES LÓGICAS Y POSIBLES MÉTODOS DE REPARACIÓN	65
2.1.1 CASO 1: SECTOR RAP (FIRMA “0XAA55”)	67
2.1.2 CASO 2: TABLA DE PARTICIONES	73
2.1.3 CASO REPRESENTATIVO 3: CORRUPCIÓN DEL SISTEMA OPERATIVO A CAUSA DE INFECCIONES POR <i>SOFTWARE</i> DEL TIPO “VIRUS INFORMÁTICO”	83
2.2 CORRUPCIONES MECÁNICAS Y POSIBLES MÉTODOS DE REPARACIÓN	119
2.2.1 CASO 1: MOTOR DE EJE CENTRAL	122
2.2.2 CASO 2: SECTORES CON DAÑO FÍSICO	132
2.2.3 CASO REPRESENTATIVO 3: PATRÓN DE RAYADO APLICADO POR EL CABEZAL DIRECTAMENTE AL PLATO MAGNETIZABLE.	139
CONCLUSIONES PARCIALES	145

CAPÍTULO 3. <i>SOFTWARE</i> “FERCUVILL V5.0” PARA LA RECUPERACIÓN DE INFORMACIÓN EN DISCOS DUROS ELECTROMECÁNICOS	146
3.1 DEFINICIÓN DE “FERCUVILL V5.0”	146
3.1.1 REQUISITOS PARA LA INSTALACIÓN Y EJECUCIÓN	147
3.2 CLASIFICACIÓN Y DESCRIPCIÓN DE LOS MÓDULOS CONSTITUTIVOS	148
3.2.1 MÓDULOS PRIMARIOS	148
3.2.2 MÓDULOS SECUNDARIOS	156
3.3 VISUALIZACIÓN DEL ENTORNO GRÁFICO DE LA INTERFAZ DE OPERACIÓN DEL <i>SOFTWARE</i> “FERCUVILL V5.0”	157
3.3.1 VENTANA DE INICIO	157
3.3.2 MÓDULO 0: J. J. B. V.	158
3.3.3 MÓDULO 1: I. C. V.	160
3.3.4 MÓDULO 2: S. V. B.	165
3.3.5 MÓDULO 3: I. C. B.	169
3.3.6 MÓDULO 4: V. H. B. V.	176
3.3.7 MÓDULO A: K. L. G.	180
3.3.8 MÓDULO B: A. J. L.	181
3.3.9 MÓDULO 5: P. A. H.	184
3.3.9.1 MÓDULO 6: S. H. B. V.	187
3.3.9.2 MÓDULO 7. H. A. A. B.	190
CONCLUSIONES PARCIALES	196

CAPÍTULO 4: MÉTODO PARA LA RECUPERACIÓN DE INFORMACIÓN (EN DISCOS DUROS ELECTROMECÁNICOS) MEDIANTE EL <i>SOFTWARE</i> “FERCUVILL V5.0”.	197
4.1 FASES DEL MÉTODO Y SU DESCRIPCIÓN	197
4.1.1 FASE 1: PRESENTACIÓN DEL OBJETO ANALIZADO	198
4.1.2 FASE 2: IDENTIFICACIÓN DEL TIPO DE FALLA PREDOMINANTE	199
4.1.3 FASE 3: ANÁLISIS SOBRE LA VIABILIDAD DE LA UTILIZACIÓN DEL <i>SOFTWARE</i> “FERCUVILL V5.0	206
4.1.4 FASE 4: UTILIZACIÓN DEL <i>SOFTWARE</i> “FERCUVILL V5.0” (MÓDULOS ESPECÍFICOS	207
4.1.5 FASE 5: COMPROBACIÓN Y ANÁLISIS DE RESULTADOS	208
4.2 APLICACIÓN DEL MÉTODO EN CASOS DE RECUPERACIÓN PROPUESTOS	209
4.2.1 CASO DE RECUPERACIÓN 1:	209
4.2.2 CASO DE RECUPERACIÓN 2:	217
4.2.3 CASO DE RECUPERACIÓN 3	230
CONCLUSIONES PARCIALES	235
CONCLUSIONES GENERALES	238
ÍNDICE DE FIGURAS	240
ÍNDICE DE TABLAS	249
REFERENCIAS	270

AGRADECIMIENTOS Y DEDICATORIAS

A la Facultad de Estudios Superiores Cuautitlán de la Universidad Nacional Autónoma de México, por brindarme la posibilidad de obtener una excelente formación académica, interdisciplinaria e integral como individuo y profesionista.

A mi madre Sara Villalobos Bravo, un pilar y símbolo de admiración en mi vida personal, a la cual, le agradezco cada uno de sus detalles diarios, su tenacidad, perseverancia y disposición a apoyarme de forma incondicional y realmente genuina. Madre, si hoy estoy en esta instancia es gracias a ti, te amo.

A mi padre Ignacio Cuevas Buendía, por impulsarme de formas varias a alcanzar y plantear objetivos sólidos, a nunca detenerme ni limitarme ante la adversidad y por promover en mí un sentido de reflexión y análisis constante. Padre, disfruta este triunfo tanto como yo, te amo.

A mis hermanos. Gracias Hilda por compartir consejos, experiencias, vivencias y sabiduría para ayudarme a hacer frente en mi toma de decisiones, esas incontables acciones hicieron de mí una mejor persona; a Víctor Hugo, por demostrar que, pese a la distancia geográfica, el interés y verdadero apoyo nunca se verán mermados, por siempre procurar en mí una ambición en pro de mi desarrollo como estudiante y para con los demás; el trabajo de tesis hoy expuesto no estaría completo sin su nombre en esta sección. A Jesús, por contribuir otorgando sus consejos y confianza, pero principalmente, por haber sentado las bases necesarias para el aprendizaje de una lengua extranjera, las cuales, fueron definitivas para entender y aprender el conocimiento desde otra y única perspectiva; a Ignacio, por su guía y contribución constantes, las cuales, procuraron en mí un invaluable interés en el área científica, de siempre cuestionar y analizar lo que me rodea.

A mi sobrina Alejandra, con la cual, he compartido y vivido momentos cruciales, los cuales, me ayudaron a afrontar de forma positiva y optimista el gran reto y esfuerzo intelectual que implica emprender esta particular forma de titulación.

A Ketty y Andy, por aceptarme y tratarme como de su familia con tan particular gentileza y cariño; el lugar en el que me consideran es igualmente recíproco.

A Patrocinio, por su característico interés, indudable e incondicional apoyo expresado de múltiples formas. Gracias por animarme a incursionar en este campo de estudio y conocimiento; hoy me siento comprometido, responsable y orgulloso de ser un ingeniero como tú.

Al ingeniero Vega, por aceptar dirigir, contribuir e involucrarse en el presente proyecto hoy ya consumado y expuesto. Además, por siempre estar dispuesto a compartir el conocimiento de forma profesional y desinteresada, con un magnífico sentido de compromiso social y docente.

Al ingeniero Cervantes, por ofrecerme sus correcciones y observaciones para conformar mi visión como ingeniero y, así mismo, por compartir su experiencia como profesionalista en el campo de la ingeniería eléctrica.

Al ingeniero Lara, por sus consejos y amable disposición al trabajo y superación continuos, así mismo, por procurar en sus estudiantes ese profundo sentido de identidad que representa ser universitario de nuestra máxima casa de estudios.

A todos aquellos que, por diferentes circunstancias no han sido mencionados, pero cuya presencia me es totalmente invaluable.

INTRODUCCIÓN

El presente proyecto de tesis toma como objeto principal de estudio al Disco Duro Electromecánico (DDE), se presentan escenarios reales de pérdida de información bajo las cuales este puede verse afectado en cualquiera de sus estructuras medulares: la mecánica y la lógica. Así mismo, se ofrecen soluciones basadas en la intervención física no invasiva del objeto mencionado y, como eje principal de investigación, la aplicación del *software* desarrollado “FERCUVILL V5.0”, ambos orientados al tratamiento (edición) efectivo de datos mediante la utilización de tecnologías físicas y virtuales, las cuales, enmarcan un método compuesto y avanzado de recuperación de información.

El *software* de diseño “FERCUVILL” recibe su nombre debido su creador y desarrollador de la presente tesis, Fernando Cuevas Villalobos. Este programa es el resultado directo del planteamiento de una solución al problema de la pérdida y/o corrupción de información en distintas unidades de almacenamiento de datos, pero en especial del DDE. La versión aquí expuesta es el compilado de sus anteriores, a las cuales, se les realizaron múltiples correcciones y mejoras ante el avance tecnológico constante de los protocolos de seguridad de la información. En su primera versión (V1.0) el programa sólo se enfocaba al restablecimiento de las propiedades de edición de los archivos y carpetas de una ubicación específica. Para la segunda versión (V2.0), además de contener las características de su antecesor, permitía al usuario identificar las características lógicas y físicas del equipo de cómputo “huésped”. La tercera versión (V3.0) implementó la primera tecnología de extracción de información interactiva entre unidades internas y externas con interfaz de conexión tipo USB y controlada mediante una barra de progreso. La cuarta entrega del *software* permitió establecer eficientemente la restauración permisos administrativos de manipulación de datos pues, de acuerdo a lo observado, este elemento se perdía inmediatamente después de que el objeto había sido alterado por la presencia de código informático malicioso. Actualmente, la quinta y más reciente versión (V5.0) presenta múltiples tecnologías para la recuperación de información y, en un intento por conservar la integridad de la misma, implementa la organización en forma de estratificaciones de módulos de operación semi-automatizados para ejecutar tareas en paralelo, es decir, una

función podrá ser ejecutada al mismo tiempo que una segunda, siempre y cuando dichas tecnologías no entren en conflicto al modificar el mismo elemento. En adición, esta versión está orientada al restablecimiento y extracción de la información cuando esta ha sufrido, de forma específica, ciertas perturbaciones en sus estructuras básicas, es decir, en los medios físicos lógicos donde existe.

Las dinámicas de operación del *hardware* y el *software* presentes en la actualidad y, aunado a la necesidad de la humanidad por preservar el conocimiento, sitúan al DDE como el principal agente presente en el almacenamiento de datos masivos, dicha categoría implica una considerable responsabilidad en el diseño físico y lógico de los distintos elementos implicados en el proceso de escritura y lectura de información. Sin embargo, existen una serie de factores internos y externos adversos que, de forma directa e indirecta y de carácter parcial y/o permanente, comprometerán a este siempre con una tendencia característica: la destrucción virtual y/o del medio en el que coexiste dicho contenido informático.

En el presente escrito desarrollado, se estudiarán los aspectos relevantes de las estructuras mecánica y lógica, así mismo, se evaluarán sus características y posibles daños a los cuales pueden ser sometidos y, en concordancia con un marco de recuperación de datos, se planteará un método lógico (en combinación con técnicas físicas) basado en un ambiente virtual de SO capaz de restablecer de la configuración base, sobre la cual, la información sea extraída y editada con seguridad.

Finalmente, los logotipos, recursos virtuales, marcas registradas y nombres de corporaciones/empresas mencionadas en el presente trabajo de tesis pertenecen exclusivamente a sus dueños legales y solo fueron utilizadas en el presente escrito para fines educativos.

OBJETIVOS

OBJETIVO GENERAL

Diseñar un *software* avanzado cuyo perfil permita la recuperación de información en unidades de Disco Duro Electromecánico (DDE) con deterioro lógico, mecánico y/o lógico-mecánico (moderado). Así mismo, plantear un método basado en un marco de recuperación de datos que considere, como eje principal, al *software* mismo.

OBJETIVOS PARTICULARES

Exponer la organización de las estructuras mecánica y lógica constitutivas del objeto de estudio analizado y, de forma inmediata, estudiar la serie de fallos y vulnerabilidades que pueden existir en estas

Establecer las dinámicas complejas de operaciones virtuales y mecánicas y, a su vez, la relación existente con el desarrollo de procesos analógicos y digitales internos orientados a la escritura y lectura de información en el DDE

Mediante el *software* propuesto, ofrecer una alternativa eficaz de extracción de información en estas unidades de almacenamiento de información cuando los métodos convencionales sean ineficaces, insuficientes u obsoletos.

Proporcionar una alternativa sólida y accesible para afrontar el fenómeno de pérdida de información y la corrupción de sus propiedades de edición y manipulación.

CAPÍTULO 1. EL DISCO DURO ELECTROMECAÁNICO

En este capítulo se describen de forma específica los componentes mecánicos y lógicos del objeto de estudio analizado, el Disco Duro Electromecánico (**DDE**), así como la relación que existe entre estos para poder realizar las operaciones de almacenamiento y extracción de datos a través de los diferentes elementos físicos y virtuales disponibles, esto con el fin de puntualizar la dinámica de funcionamiento y procesos implicados a lo largo de este fenómeno.

1.1 RESEÑAS HISTÓRICAS

La tendencia en estos dispositivos de almacenamiento de datos ha sido siempre orientada a la expansión de la capacidad de almacenamiento de datos, es decir, del espacio virtual para poder guardar información, para ello han sido modificados en su diseño físico, componentes, dimensiones y por supuesto su eficiencia de funcionamiento al igual que su lógica de programación; esto se ha logrado gracias al trabajo y dedicación de múltiples compañías a lo largo de la historia. A continuación se mostrarán aquellos eventos cronológicos destacables en dicho proceso.

RAMAC 1 (Sistema de Contabilidad con Memoria de Accesos Aleatorio), diseñado por la empresa **IBM** (“**International Business Machines**”) [39], es oficialmente el primer disco duro electromecánico registrado, introducido en la computadora modelo **IBM 350** el 13 de Septiembre 1956, su capacidad total de almacenamiento era de **5 MB** (“**Mega Bytes**”) y contaba con una masa de 1000 kilogramos; la pureza del medio la lograba mediante el uso de válvulas de vacío, en tanto que el control lógico se establecía mediante una consola independiente [2].

IBM 1301, diseñado en el año de 1961, su capacidad de almacenamiento era prácticamente 5 veces la de su homólogo previo, el RAMAC 1, contando con un valor de 24 MB, este modelo es de especial importancia debido a que el concepto de su mecanismo “actuador” se sigue utilizando en la actualidad, Este permitía la lectura y escritura de datos a través de

cabezas “deslizantes” e independientes que cubrían ambas caras del plato que, mediante movimientos horizontales, podían posicionarse en la localidad deseada [21].

IBM 1311, surge en el año de 1962, adopta en arreglo de “paquetes de discos removibles”, su antecesor, el IBM 1311 solamente podía maniobrar con un paquete permanente, contaba con múltiples paquetes de platos intercambiables según se requiriera almacenar mayor información o leer la anteriormente guardada, la capacidad de cada uno de estos se encontraba en el rango de los 2 MB [40].

IBM 3340, es presentado de forma oficial en el año de 1973, el nombre código con el que se le conoció fue “**Winchester**” y estaba designado para formar parte del equipo **IBM System/370**; contaba con un sistema de paquetes de discos removibles al igual que la serie 2310, 2321 y 330, sin embargo, el IBM 3340 poseía un juego de cabezas de lectura y escritura igualmente desmontables y ajustadas en los paquetes de platos, su tiempo de acceso era de 25 milisegundos a velocidad de transferencia de 885 **KB/s** (“**Kilo-Bytes sobre segundo**”). La capacidad de almacenamiento máxima fue de 70 MB.

El término de “**Winchester**” es debido a que estaba originalmente diseñado con un par de módulos de 30 MB cada uno, el arreglo “30-30” emulaba al arma de fuego; si bien la capacidad superó los 60 MB el término para referirse a este continuó de forma coloquial [88].

IBM 3380, el diseño nace en 1980 pero es hasta 1981 cuando esta versión sale al mercado (debido a fallos mecánicos), este DDE es de especial interés debido a que es el primero en medir su almacenamiento en Giga-Bytes (**GB**), cada paquete de platos tenía una capacidad final de 2.52 GB y podían funcionar en arreglo de cadena, es decir, este soportaba hasta un total de 9.3 GB; contaba con unidades de control independientes que podían maniobrar con 8 unidades de cadena IBM 3380 completas. En cuanto a sus tiempos, este dispositivo incorporó la tecnología de “película fina” (permitía una lectura y escritura más fluida) con una velocidad de transferencia de 3MB por segundo con un tiempo de acceso de 16 milisegundos [21, 88].

ST-506, diseñado por la empresa **SEAGATE** [79, 28] e introducido al mercado en el año de 1981. Es el primer DDE de 5.25 pulgadas de tamaño con una capacidad de almacenamiento de 5MB que funcionaba con un “motor a pasos” [46].

RO-352, creado por la empresa **Rodime** [33] en el año de 1983, es el primer DDE con un tamaño de 3.5 pulgadas, justo el tamaño que se usa en la actualidad para las unidades internas en equipos de escritorio; construido con 4 cabezas de lectura y escritura para controlar un arreglo de 306 cilindros, su diseño permitía una capacidad de almacenamiento de datos total de 11 MB [33].

CP340 y **CP3022**, ambas unidades de DDE pertenecen a la empresa **Conner** [23, 48, 98], manufacturados en el año de 1988. El CP340 incorpora el sistema **VCM (“Voice Coil Motor”)**; dicha tecnología permite mover al actuador completo mediante la interacción de un campo magnético fijo y otro generado a partir de la energización de una bobina unida al cabezal del actuador mismo. En tanto que el modelo CP3022 soportaba una altura de 1 pulgada dentro de una carcasa de 3.5 pulgadas. Ambos dispositivos podían almacenar hasta de 20 MB [83].

La empresa Seagate compite con el lanzamiento del primer DDE de 7200 **RPM** (“**Revoluciones Por Minuto**”) y para el año 2000 permite hasta 15000 RPM [49], típicamente estos últimos se utilizan para equipo llamados “servidores” [15] los cuales permiten controlar, mediante el uso de un *software*, a múltiples sistemas interconectados para la ejecución de tareas específicas.

IBM Deskstar 75GXP, este dispositivo es producido y mercantilizado el 15 de Marzo del año 2000, cuenta con una capacidad de almacenamiento de datos de 75 GB, este DDE equivalía a tener la capacidad de 10 computadoras de la época; giraba a 7200 RPM con una velocidad de transferencia de 37 MB/s y tan sólo 680.38 gramos [24].

A partir de este evento histórico es que la compañía Seagate comienza a crecer en el mercado de producción y distribución de unidades de DDE con la generación del modelo **Barracuda 180**, este mismo, contenía en efecto 180 GB de almacenamiento de datos; para el año 2005, la serie **Barracuda 7200.9** permite hasta 500 GB con una interfaz de acceso sostenida de 3 GB/s (“**Giga Bytes sobre segundo**”) [34], la serie **Barracuda 7200.10**,

desarrollada en 2007, ofrece una capacidad mínima de 80 Gb y máxima de 750 GB con una tecnología de grabado perpendicular; para el **Barracuda 7200.11**, creado en 2009, establece una capacidad base de 160 GB y máxima de 1.5TB (“**Tera-Bytes**”), por otra parte, la serie **Barracuda 7200.12**, (igualmente diseñada a finales del 2009), no está diseñada para superar en capacidad de almacenamiento, sino en velocidad de transferencia de datos, (valor de 6 GB/s), en comparación con los modelos 7200.10 y 7200.11 que sólo admiten 3GB/s [81].

Barracuda Serie LP, comercializado en 2009, es un DDE creado específicamente para soportar grandes capacidades de almacenamiento de datos con valores mínimos desde los 500 GB hasta los 2 TB, la velocidad del motor es de 5900 RPM. Surge de la necesidad de reducir los valores de temperatura a la salida del dispositivo, así pues, cuenta con una interfaz de transferencia de 3GB/s [81].

En el año 2015, las compañías **TOSHIBA** [90] y Seagate son las que han presentado avances considerables en cuando al rendimiento, eficiencia y versatilidad en la producción en masa para unidades de DDE, siendo el caso de TOSHIBA al presentar el **MQ03ABB300** con 2.5 pulgadas de tamaño y una capacidad de almacenamiento de 3.0 TB [90]; en tanto que la compañía Seagate ha diseñado el **Archive HDD** de 3.5 pulgadas y una capacidad máxima de 8TB con una interfaz de 6GB/s ; de acuerdo a Seagate [80], este DDE incorpora la tecnología **SMR** en la cual la información es guardada en forma de traslapes escalonados que permiten el aumento del 25% de la capacidad máxima en un DDE de mismas dimensiones sin alterar la información consecutiva, aumentando así la eficiencia de almacenamiento con un mismo consumo energético.

FABRICANTES

Los fabricantes de estos dispositivos históricamente han realizado maniobras de mercadotecnia y/o fusiones para poder implementar mejores tecnologías, o bien, para evitar la desaparición de las empresas mismas ante crisis económicas.

En los últimos 27 años es que estos eventos han tenido mayor impacto, son cambios que primordialmente están orientados al aumento de la capacidad de almacenamiento, velocidad de lectura y escritura de datos así como el factor de forma, es decir, el tamaño y

distribución física que el DDE tiene para su respectivo uso. Estos cambios han establecido a las empresas que predominan en la actualidad. En la tabla 1.1 se presenta de forma cronológica aquellas fusiones representativas y los eventos que fueron influyentes en dicho proceso [3, 43].

AÑO	EVENTO	COMPAÑÍA RESULTANTE
1988	Western Digital adquiere la división de fabricación de discos duros de Tandom .	WESTERN DIGITAL.
1989	Seagate adquiere la línea de discos de alta calidad de Control Data .	SEAGATE.
1990	Maxtor adquiere a MiniScribe , permite crear DDE de gama baja.	MAXTOR.
1994	Quantum adquiere la división de almacenamiento de Digital Equipment , generado la línea “ProDrive”, la cual produce discos de alta calidad.	QUANTUM.
1995	Conner Peripherals anuncia su fusión con Seagate .	SEAGATE.
1996	JST se fusiona con Atari para la producción en masa de discos, sin embargo, Atari es vendida a Hasbro en 1998 y JST desaparece.	

2000	Maxtor adquiere la línea Quantum.	MAXTOR.
2003	Hitachi adquiere en su mayoría a la línea de producción de discos de IBM.	HITACHI GLOBAL STORAGE TECHNOLOGIES.
2003	Western Digital adquiere a Read-Rite Corporation.	WESTERN DIGITAL.
AÑO	EVENTO	COMPAÑÍA RESULTANTE
2005	Seagate adquiere la línea Maxtor.	SEAGATE.
2007	Western Digital adquiere a Komag U.S.A.; el cual fabricaba el material magnético que recubre a los platos internos.	WESTERN DIGITAL.
2009	Toshiba adquiere la línea de producción de discos de la empresa Fujitsu.	TOSHIBA.
2011	Western Digital adquiere a Hitachi Global Storage Technologies	WESTERN DIGITAL.
2011	Seagate adquiere a Samsung	SEAGATE.
2015	Seagate distribuye en el mercado el DDE Archive HDD con capacidad de 8TB.	SEAGATE.

Tabla 1. Evolución y fusión de fabricantes de dispositivos de DDE.

En función de la tabla 1 se puede establecer entonces que los fabricantes predominantes en la actualidad son:

- SEAGATE.
- WESTERN DIGITAL.
- TOSHIBA.

1.2 DEFINICIÓN DEL DISCO DURO ELECTROMECAÁNICO

Se le denomina así al dispositivo mecánico, eléctrico y electrónico capaz de almacenar información digital mediante el uso de señales magnéticas dirigidas estratégicamente sobre discos rígidos y/o platos magnetizables en un ambiente controlado. Dicho dispositivo pertenece al grupo de familias lógicas denominadas como “no volátiles”, es decir, los datos contenidos en este existen de forma permanente aun cuando no se encuentre conectado a alguna fuente de alimentación eléctrica constante.

FUNCIONAMIENTO

Existe un motor de **C.D.** (“**Corriente Directa**”) principal sobre el cual se encuentran asidos los platos y/o discos rígidos los cuales giran a una velocidad constante; dependerá de la capacidad en RPM del motor la velocidad angular de los platos; sobre estos se guarda la información a manera de señales magnéticas, estos platos a su vez están hechos de aluminio (**Al**) o cristal pulidos y recubiertos por un material basado en cobalto (**Co**). Los procesos de lectura y escritura son logrados a partir de elementos llamados “cabezas” que son capaces de tanto emitir (cabezas de escritura) como de recibir (cabezas de lectura) valores almacenados/enviados en los discos rígidos. Las cabezas están conectadas a un dispositivo llamado “deslizador” el cual brinda soporte y estabilidad a las cabezas cuando están efectuando sus operaciones; el deslizador está igualmente sostenido por una estructura completa llamada “brazo”, este último constituye básicamente la mayoría del soporte mecánico, es decir, admite el estrés producido por los movimientos de posicionamiento provenientes en parte de los rodamientos pero principalmente por el dispositivo VCM, este último está constituido por una bobina suspendida entre un par de campos magnéticos fijos, la interacción de campos genera el movimiento específico requerido por el DDE para colocarse sobre el “cilindro”, luego en la “pista” y finalmente en el “sector” adecuados. La

estructura completa recibe el nombre de “actuador”, el cual puede estar configurado con respecto a los platos rígidos de forma horizontal (paralelo) o bien de forma vertical (ortogonal) [4].

El elemento “preamplificador” es el **CI** (“Circuito Integrado”) interno encargado de la transformación de señales magnéticas a digitales y viceversa, dicho circuito está soldado y/o adherido a un costado del actuador y conectado a través de un cable de datos plano que comunica las señales provenientes de las cabezas con la **TCI** (“Tarjeta de Circuito Impreso”) (ver página 11).

1.3 ESTRUCTURAS

Para abordar el estudio del DDE es necesario categorizar sus diferentes elementos constitutivos en secciones que permitan una descripción precisa para establecer las dinámicas de funcionamiento físicas (estructura mecánica) y virtuales (estructura lógica) que, a su vez, dictaminan los procesos de escritura y lectura de datos.

Habiendo mencionado lo anterior, la clasificación modelo que se seguirá para comprender dicho estudio está expresado en la tabla 2 con el siguiente arreglo:

DISCO DURO ELECTROMECAÁNICO	
ESTRUCTURA MECÁNICA	ESTRUCTURA LÓGICA
<ul style="list-style-type: none"> • CARCASA Y CUBIERTA. 	<ul style="list-style-type: none"> • SECTORES, CLÚSTERS, PISTAS, ZONAS, CILINDROS Y SISTEMA “SERVO”.
<ul style="list-style-type: none"> • MOTOR DE CORRIENTE DIRECTA DE EJE CENTRAL. • PLATOS. 	<ul style="list-style-type: none"> • SECTOR DE ARRANQUE MAESTRO.
<ul style="list-style-type: none"> • DISPOSITIVO ACTUADOR. 	<ul style="list-style-type: none"> • TABLA DE PARTICIONES.
<ul style="list-style-type: none"> • TARJETA DE CIRCUITO IMPRESO (TCI). • INTERFAZ DE CONEXIÓN. 	<ul style="list-style-type: none"> • SISTEMA DE ARCHIVOS.

Tabla 2. Elementos mecánicos y lógicos estructurales del DDE.

1.3.1 ESTRUCTURA MECÁNICA

Este tipo de estructura se define como aquella que permite contener, organizar y relacionar a todos los elementos físicos internos y externos del DDE permitiendo así el funcionamiento armónico de los mismos [20].

El término “factor de forma” es un criterio de diseño que hace referencia a la distribución física y, en consecuencia, las dimensiones finales que el DDE tendrá como modelo. A lo largo de la historia se han presentado múltiples factores de forma, los cuales tuvieron la tendencia de verse reducidos, en tanto que la capacidad de almacenamiento ha aumentado [4].

Para los fines del presente proyecto de investigación, se analizará exclusivamente el factor de forma de 3.5 y 2.5 pulgadas, es decir, medidas estándares para equipos de escritorio y portátiles, respectivamente.

A continuación, en la tabla 3, se presenta la división modelo utilizada para abordar el estudio de la estructura mecánica:

ESTRUCTURA MECÁNICA	
ARREGLO EXTERNO	ARREGLO INTERNO
CARCASA Y CUBIERTA.	MOTOR DE CORRIENTE DIRECTA DE EJE CENTRAL.
TARJETA DE CIRCUITO IMPRESO (TCI).	PLATOS.
INTERFAZ DE CONEXIÓN.	DISPOSITIVO ACTUADOR.

Tabla 3. Subdivisión de los elementos mecánicos del DDE.

ARREGLO EXTERNO

CARCASA Y CUBIERTA

Estos elementos conforman la totalidad del cuerpo o “armazón” del DDE permitiendo crear un ambiente controlado (control de contaminación y flujo de aire) óptimo para la rotación del motor y de los platos unidos a este, al igual que el movimiento del actuador completo por sobre encima de los platos.

La carcasa es el elemento sobre el cual se soporta el motor de C.D. y sus contactos de alimentación; al igual que los orificios de ventilación y entradas de conexión de los elementos internos, es decir, los contactos del actuador hacia la TCI.

La cubierta es básicamente un elemento protector que termina por sellar la carcasa en su parte superior mediante el uso de tornillos y gomas adhesivas. Esta es la encargada de controlar el flujo de aire producido por la velocidad angular del motor y platos que acontecen en el DDE, su importancia radica en establecer el flujo correcto de este fluido a través de un filtro de purificación, dicho patrón específico está diseñado de tal forma que permita un ambiente libre de impurezas pero igualmente suficiente para brindar sustentación al dispositivo actuador y, principalmente, al cabezal cuando se encuentra funcionando.

Así mismo, en su parte superior, la cubierta brinda los datos de placa de fabricación relevantes acerca del DDE. Esta información es crucial para conocer las capacidades y rangos de operación bajo los cuales el dispositivo trabaja, así como para conocer los criterios de compatibilidad necesarios a cumplir para establecer una recuperación de datos óptima.

El diseño, información y distribución de los datos de placa varían de acuerdo a cada fabricante. En las figuras 1 y 2 se muestran, respectivamente, la cubierta y la carcasa para un DDE.

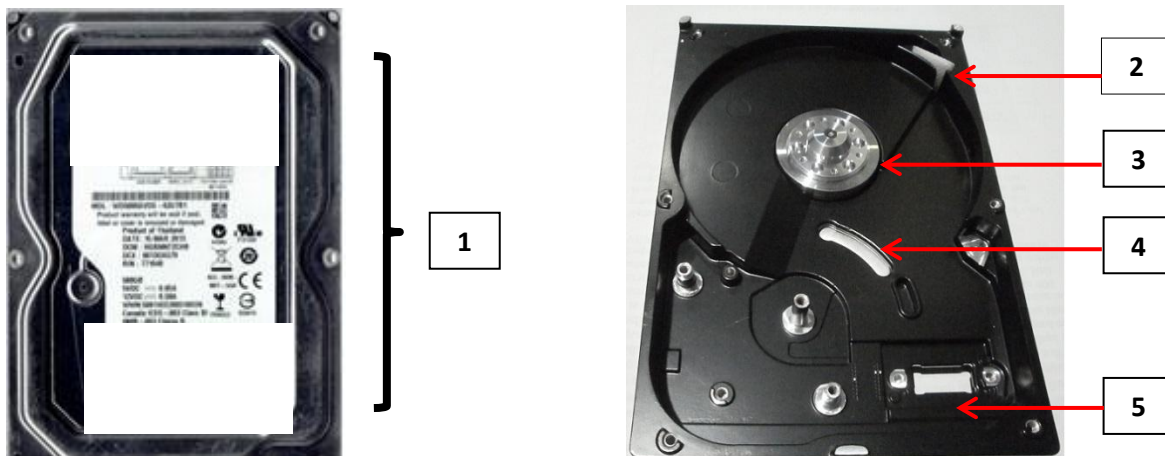


Figura 1. Cubierta y datos de placa de un DDE.

Figura 2. Elementos internos de la carcasa.

En la tabla 4 se describen los elementos especificados en las figuras 1 y 2, respectivamente:

NÚMERO	DESCRIPCIÓN
1	DATOS DE PLACA.
2	FILTRO DE AIRE.
3	MOTOR.
4	CARCASA.
5	ORIFICIO DE CONEXIÓN DEL ACTUADOR.

Tabla 4. Identificación de los elementos de la carcasa y cubierta del DDE.

TARJETA DE CIRCUITO IMPRESO (TCI)

Este elemento se define como aquel mecanismo de control eléctrico y electrónico, comunicación e interpretación de datos sobre dispositivos dinámicos y estáticos mediante la utilización de CI asociados por cada elemento existente.

El control de los dispositivos se lleva a cabo mediante la utilización de los procesos de lectura y escritura de instrucciones lógicas, las cuales a su vez realizan la subrutina directa sobre el elemento controlado. Las instrucciones lógicas de operación son almacenadas previamente en bancos de memoria no volátiles tipo **ROM** (“Read Only Memory”), es

decir, “Memoria de Sólo Lectura”. El contenido de estos bancos no puede ser alterado debido a que no existen entradas de escritura en su estructura, o bien, se encuentran deshabilitadas, entonces solamente cuenta con salidas de datos. Por otra parte, para ejecutar y almacenar temporalmente datos del *firmware* y analizar futuros datos a leer utiliza la memoria **RAM** (“**Random Access Memory**”), es decir, “Memoria de Acceso Aleatorio” [55].

ORGANIZACIÓN ESTRUCTURAL

Los componentes constitutivos de la TCI pueden ser expuestos de acuerdo a su distribución física tal y como se muestra en la tabla 5.

DISTRIBUCIÓN FÍSICA	
CIRCUITOS INTEGRADOS.	<ul style="list-style-type: none"> • UNIDAD MICROCONTROLADORA (UMC)/UNIDAD CENTRAL DE PROCESAMIENTO (UCP). • MEMORIAS (RAM, ROM). • CONTROLADOR VCM.
CONTACTOS.	<ul style="list-style-type: none"> • MOTOR. • CABEZAL.
MÓDULOS DE PROTECCIÓN.	<ul style="list-style-type: none"> • DIODOS SVT. • SENSOR DE SOBRECORRIENTE.

Tabla 5. Distribución física de los componentes de la TCI.

Los componentes expresados en la tabla 5 dependen del diseño de cada fabricante, así como su posición, existencia y distribución. Para los fines del presente proyecto, se utilizó una TCI perteneciente a un DDE de la marca Seagate con capacidad de 500 GB como modelo principal, así mismo, se mencionan las definiciones para cada uno de los elementos internos constitutivos del elemento mencionado.

A continuación, en la figura 3, se observa la TCI modelo utilizada y, en complemento, en la tabla 6 se identifican los componentes primeramente citados en la tabla 5 con el arreglo siguiente:

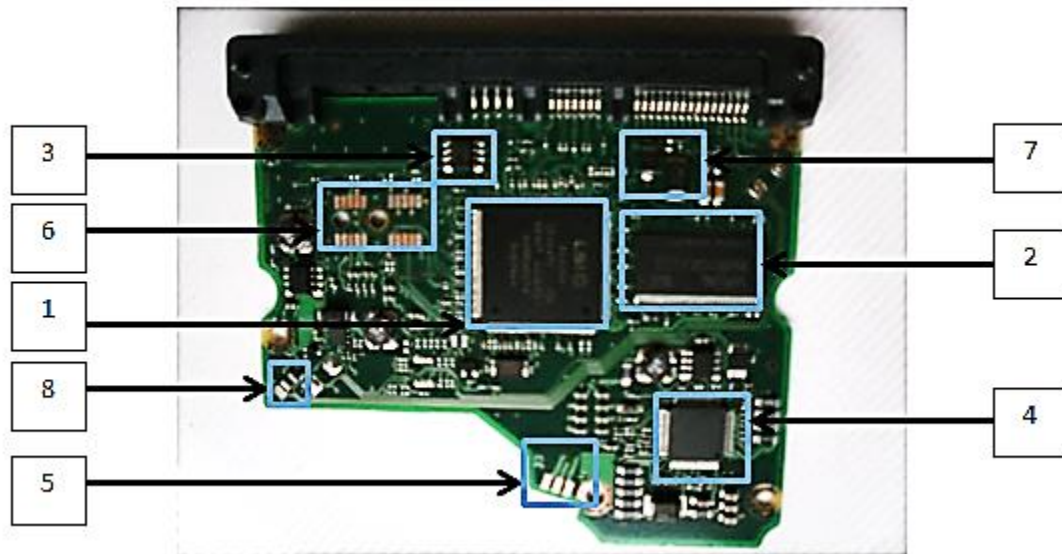


Figura 3. Componentes de la TCI de un DDE con interfaz SATA.

NÚMERO	DESCRIPCIÓN
1	UNIDAD MICROCONTROLADORA.
2	MEMORIA RAM.
3	MEMORIA ROM.
4	CONTROLADOR VCM.
5	CONTACTOS DEL MOTOR.
6	CONTACTOS DEL CABEZAL.
7	DIODOS SVT.
8	SENSOR DE IMPACTO.

Tabla 6. Identificación de los componentes de la TCI.

Se procede entonces con la descripción de los elementos presentes en la tabla 1.6 en el mismo orden en que aparecen.

UNIDAD CENTRAL DE PROCESAMIENTO (UCP)

También conocida como UMC (“Unidad Micro Controladora”); es el circuito de mayor tamaño físico en la TCI, es el encargado de realizar todos los cálculos de control referentes a los canales de lectura y escritura de datos. En conjunto con el circuito preamplificador, transforma las señales analógicas provenientes de las cabezas en señales digitales cuando se

encuentra operando el modo de lectura y, a su vez, codifica señales digitales en señales analógicas cuando se habilita el modo de escritura.

La capacidad de la UCP para interpretar datos de escritura y lectura es lograda gracias a la implementación de puertos de **E/S (“Entrada/Salida”)**. Dichos puertos establecen el control total al permitir la transferencia de instrucciones y datos desde y hacia la TCI, tanto con los demás CI adyacentes como con la interfaz de conexión existente, es decir, sea SATA o IDE según corresponda. Para este DDE la interfaz de conexión es SATA (ver página 18). Para los fines del presente proyecto de investigación, sólo la tecnología tipo SATA es estudiada.

MEMORIA RAM

Se utiliza un chip tipo **DDR SDRAM (“Dual Data Rate, Synchronous Dynamic Random Access Memory”)**, es decir, “Memoria Síncrona Dinámica de Acceso Aleatorio con Transmisión Doble de Datos”. Esta memoria tiene un par de funciones específicas, la primera de ellas es la de proporcionar un espacio de almacenamiento temporal para guardar archivos que se han abierto y, en un intento por agilizar la velocidad de transferencia de datos, estos puedan ser accedidos nuevamente si son requeridos por el usuario; la segunda función está orientada a la capacidad de almacenar instrucciones de arranque provenientes del módulo *firmware* controladas por la UMC para ejecutar las líneas de código de reconocimiento del DDE ante el **BIOS (“Basic Input Output System”)**, es decir, “Sistema Básico de Entrada y Salida”. La memoria utilizada por la TCI modelo corresponda a una SAMSUNG DDR con una capacidad de 32 MB.

MEMORIA ROM

Este circuito, en conjunto con el **AS (“Área de Servicio”)** (ubicada en un espacio específico reservado de los platos internos y grabado de forma magnética con patrones de control establecidos por cada fabricante) son los encargados de guardar, leer y ejecutar el módulo *firmware*.

El **módulo *firmware*** se define como aquel *software* interno cuyo objetivo es relacionar los dispositivos físicos y sus señales resultantes con aquellas instrucciones lógicas orientadas,

mediante el uso del control digital, al reconocimiento, interpretación, jerarquización y ejecución de tareas específicas que el dispositivo completo (DDE) responde para establecer una armonía de funcionamiento tal que permita operar dentro de ciertos criterios de estabilidad.

Para la TCI, el módulo *firmware* está ubicado en una memoria digital típicamente ROM; en dicha memoria se almacenan los siguientes parámetros:

1. Archivos de registro del **S.M.A.R.T.** (“**Self-Monitoring, Analysis and Reporting Technology**”), es decir, “Tecnología de Auto-monitoreo, Análisis y Reporte”.
2. Control eléctrico del motor (generación de pulsos).
3. Información sobre la configuración y arreglos del DDE.
4. Número de cabezas.
5. Habilitación e inhabilitación de las cabezas.
6. Cantidad de sectores totales mediante el sistema **CCS** (“**Cilindro-Cabeza-Sector**”).
7. Mapa de sectores y tabla de asignación de direcciones lógicas por cabeza.
8. Delimitación entre el AS y el AU (“**Área de Usuario**”).

En cuanto al otro módulo *firmware* que se encuentra almacenado en los platos, los parámetros de operación contenidos son:

1. Reportes de registro del S.M.A.R.T. y contraseñas de acceso al DDE.
2. Tabla de asignación de defectos.
3. Tabla de reasignación de direcciones lógicas.

Cuando el DDE es energizado, la UMC accede al código *firmware* de la memoria ROM en la TCI y comienza a ejecutar los parámetros de reconocimiento citados, los compara entonces con los datos del módulo *firmware* almacenados en los platos y, si estos coinciden, comienza la secuencia de comandos que permiten reconocer exitosamente el DDE conectado; primeramente ante el *software* BIOS y en segundo lugar ante el **SO** (“**Sistema Operativo**”) asociado (ver página 81).

CONTROLADOR VCM

Este circuito electrónico es el que tiene un mayor consumo energético de toda la TCI, esto debido a que tiene un par de funciones primordiales:

1. Permite el control de la rotación del motor.
2. Establece el control del actuador completo y, por lo tanto, el movimiento de las cabezas.

Debido al potencial de consumo del circuito, su núcleo interno está diseñado para operar a temperaturas de 100°C/212°F sin verse afectado en su desempeño [1, 2, 77].

CONTACTOS

Existen un par de zonas de contactos con la TCI y la carcasa. Como ya se ha mencionado anteriormente, la comunicación de los dispositivos internos con la lógica de programación de los circuitos integrados externos es lograda a partir de la comunicación permanente entre dos o más elementos de una zona determinada; así pues, los distintos modelos de TCI utilizan puntos de contacto hechos de **Cobre (Cu)** en el motor y el cabezal, estos, basados en un modelo de alta resistencia a la oxidación bajo operaciones a bajas temperaturas.

DIODOS SVT

Estos circuitos de protección reciben su nombre de las siglas **SVT** (“Supresor de Voltaje Transitorio”) y son los encargados de detectar sobrecargas de energía eléctrica en la TCI; la causa principal por la cual se presenta este fenómeno es típicamente un fallo en la fuente de alimentación y/o cortes repentinos los cuales hacen que existan niveles de tensión y corriente fuera del rango nominal de operación.

El funcionamiento de este dispositivo consiste en provocar un corto-circuito entre las terminales de alimentación y tierra cuando existe cierta corriente de falla que potencialmente puede destruir la placa y los elementos conectados a ella, entonces el diodo literalmente funde un puente interno que envía dicha energía a un punto seguro donde no pueda causar daños superiores. En la TCI modelo se utilizan un par de este tipo protecciones para valores de 5V y 12V respectivamente.

SENSOR DE IMPACTO

Este dispositivo de control físico es capaz de detectar movimientos y vibraciones que comprometen la integridad de los elementos internos de la carcasa.

El dispositivo se acciona cuando detecta alguna fuerza externa, o bien, algún movimiento oscilatorio (proveniente del motor y/o el actuador) que alteran el estado de equilibrio del DDE, el cual, idealmente debería de funcionar solamente de forma paralela a la superficie de contacto, sin embargo es posible encontrarlos en posiciones perpendiculares; especialmente aquellos que funcionan como unidades externas.

La protección actúa entonces enviando una señal eléctrica al controlador VCM el cual, sin esperar respuesta del MCU ejecuta las siguientes funciones:

1. Coloca el actuador en la zona de estacionamiento.
2. Anula la alimentación eléctrica hacia el motor.

Esta tecnología permite suponer que el DDE ya no se encuentra más es una superficie estable, por ello protegerá a los platos de un contacto continuo en contra del actuador lo cual provocaría una pérdida de información definitiva.

El diseño y posición de los sensores depende del fabricante y proceso de manufactura, se implementan dos sensores para proteger tanto el interior como el exterior del DDE según corresponda. Para la TCI analizada sólo contempla uno de ellos en su diseño [1, 2, 77].

Continuando con el arreglo externo, la interfaz de conexión, debido a la perspectiva, no puede ser vista en la figura 1.3, esta conforma la comunicación medular entre el DDE y la computadora asociada a este.

INTERFAZ DE CONEXIÓN

La TCI permite la comunicación interna de sus circuitos a través de “pistas” y/o ranuras hechas de material semiconductor, sin embargo necesita establecer comunicación externa tanto para enviar y recibir datos como para alimentarse eléctricamente.

La **interfaz de conexión** se define entonces como aquel circuito físico que permite la emisión y recepción de valores eléctricos (alimentación) y digitales (información) a través cables conductores conectados a una placa base perteneciente a un sistema computacional.

La interfaz presente en la TCI mostrada es del tipo **SATA** (“**Serial Advanced Technology Attachment**”), es decir, “Tecnología de Conexión Serial Avanzada”. De acuerdo a sus datos de placa, tiene una velocidad de 3Gb/s con alimentación eléctrica de 5V y 12V. El diagrama estructural para datos y energización puede observarse en las figuras 4 y 5, respectivamente [94].

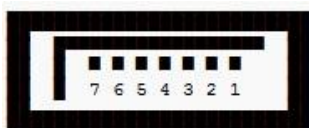


Figura 4. Conector SATA de datos.

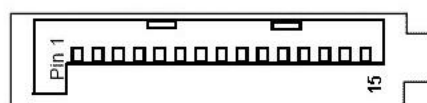


Figura 5. Conector SATA de alimentación.

Respectivamente, en las tablas 7 y 8 se colocan los valores para cada uno de los nodos de conexión mostrados en las figuras 4 y 5. Estos valores son universales y no dependen del fabricante o desarrollador de la TCI [5].

SATA (DATOS)			
NODO	NOMBRE	ESTADO DEL DISPOSITIVO	ESTADO DEL SERVIDOR
1	GND.	PUESTO A TIERRA.	PUESTO A TIERRA.
2	(A+).	TRANSMITE.	RECIBE.
3	(A-).	TRANSMITE.	RECIBE.
4	(GND).	PUESTO A TIERRA.	PUESTO A TIERRA.
5	(B+).	RECIBE.	TRANSMITE.
6	(B-).	RECIBE.	TRANSMITE.
7	(GND.)	PUESTO A TIERRA.	PUESTO A TIERRA.

Tabla 7. Valores de nodos para el conector SATA de datos.

SATA (ALIMENTACIÓN)		
NODO	VALOR	DESCRIPCIÓN
1	(+3.3V).	VOLTAJE.
2	(+3.3V).	VOLTAJE.
3	(+3.3V).	VOLTAJE DE RESPALDO.
4	(GND).	PUESTA A TIERRA.
5	(GND).	PUESTA A TIERRA.
6	(GND).	PUESTA A TIERRA.
7	(+5V).	VOLTAJE DE RESPALDO.
8	(+5V).	VOLTAJE.
9	(+5V).	VOLTAJE.
10	(GND).	PUESTA A TIERRA.
11	(GND).	TIERRA DE RESPALDO.
12	(GND).	PUESTA A TIERRA.
13	(+12V).	VOLTAJE DE RESPALDO.
14	(+12V).	VOLTAJE.
15	(+12V).	VOLTAJE.

Tabla 8. Valores de nodos para el conector SATA de alimentación.

De acuerdo a lo expuesto anteriormente, es posible indicar que el arreglo externo abarca fundamentalmente los siguientes campos:

1. Proporcionar protección física a los elementos internos sensibles.
2. Otorgar información sobre los datos de placa necesarios para conocer las condiciones nominales de operación y criterios de compatibilidad.
3. A partir de la TCI, proporcionar una plataforma de comunicación y funcionamiento que relaciona ambas fases del *software* operacional, es decir, la lógica de programación del DDE (*firmware*) con el *software* básico BIOS del computador o servidor utilizado.

Debido a que este arreglo no puede constituir por si solo una estructura mecánica completa y, partiendo de que su característica fundamental es la del control, entonces es igualmente necesario identificar y definir aquellos elementos pertenecientes al arreglo interior.

ARREGLO INTERNO

MOTOR DE CORRIENTE DIRECTA DE EJE CENTRAL

Se le llama exactamente así debido a su diseño, este dispositivo está completamente soportado en la base de la carcasa pero es sostenido por un buje o eje fijo que funciona a partir de rodamientos que permitan el libre movimiento circular del motor sin que se produzcan perturbaciones y/o movimientos oscilatorios provenientes tanto del motor mismo (vibraciones) como de fuerzas externas.

CARACTERÍSTICAS DE DISEÑO Y OPERACIÓN

Este dispositivo cuenta con ciertas cualidades que le permiten a la TCI implementar un control digital óptimo para efectuar los procesos de escritura y lectura de datos, las cuales son:

1. Tiene un bajo consumo eléctrico, típicamente estos dispositivos son alimentados con 12V y pueden alcanzar velocidades de entre 3600 RPM hasta 15000 RPM según el modelo y tipo de DDE utilizado.
2. Funciona con CD, por ello puede ser gobernado lógicamente ante la necesidad de una repentina pérdida del potencial de alimentación y/o una detención por parte del controlador VCM a partir de la supresión de impulsos.
3. Proporciona una velocidad constante y con ello uniformidad de lectura-escritura, esta última asegura que la información guardada en un sector específico por el cabezal en forma de bits pueda ser accedida nuevamente en el modo de lectura.
4. Conjunto con la carcasa y cubierta (y mediante la implementación de dispositivos “espaciadores”), permite crear un control de flujo de aire entre cada uno de los platos (cuando el DDE cuenta con más de uno) y sus respectivas cabezas, con ello es posible evitar de forma efectiva el fenómeno denominado como “impacto del cabezal” el cual es la condición de mayor influencia relacionada a la pérdida de información.
5. Su diseño lógico para el control preciso de la velocidad de operación permite la reducción y, en términos prácticos de funcionamiento, la atenuación de la señal de

ruido, la cual se produce por la naturaleza eléctrica de los componentes de la TCI con la generación de valores lógicos por parte de los CI de control asociados.

La señal de ruido puede ocasionar, fundamentalmente, la siguiente condición:

- Producción de valores lógicos indeseables que afecten el proceso de escritura mediante la alteración de la densidad de bits, es decir, la cantidad de bits que existen guardados en una determinada área física del plato.

En la figura 6 y tabla 9 se muestran, respectivamente, los componentes del motor, a su vez, es posible observar el eje central y el anillo de soporte, este último está colocado entre el motor mismo y la carcasa, su función es la de permitir la distribución uniforme de las vibraciones producidas.

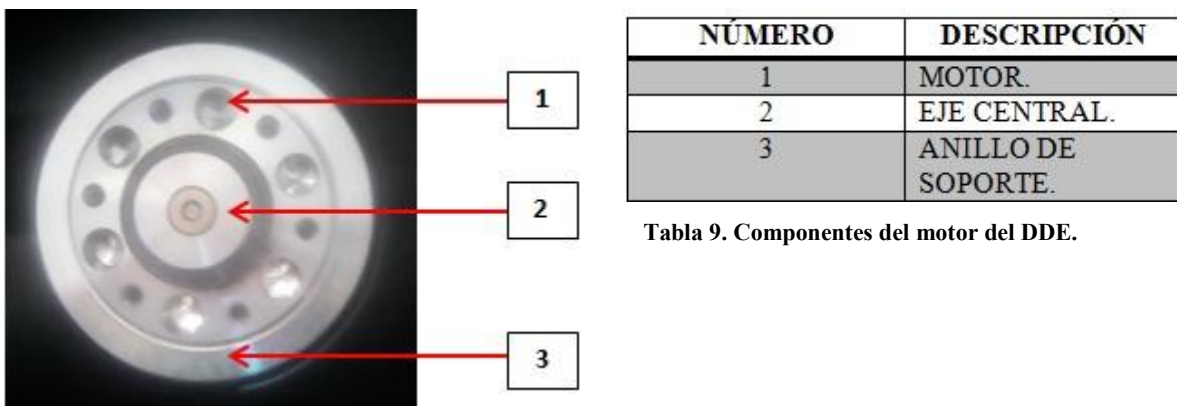


Figura 6. Motor, base y eje central de DDE.

Es importante enfatizar que cualquier manifestación sea de origen lógico (producida por la señal de ruido y/o fallo en el CI asociado) o de origen mecánico (fuerza externa aplicada al DDE durante su respuesta permanente), provocará un fallo en la velocidad del motor, lo cual, se traduce en un deterioro en la razón de bits expresada en los platos internos.

La razón de bits, la cual se mencionó anteriormente, se define como la comparación de la información escrita en contra de la información leída en un espacio físico delimitado en los platos internos en un tiempo conocido, así pues, si la velocidad de rotación es diferente en el DDE cuando se escribieron los datos de cuando fueron leídos nuevamente el cabezal no estará en la misma posición y, por lo tanto, la razón de bits será diferente; es entonces que sucede una corrupción de la información, esta es dañada, sobre-escrita y/o inaccesible por cualquier método de lectura disponible.

CLASIFICACIÓN

Estos dispositivos son ordenados de acuerdo a su tecnología de rodamientos y, en consecuencia, de acuerdo a su capacidad de eliminación de movimientos oscilatorios aleatorios no compensados los cuales no sólo afectan al motor mismo sino a los platos y cabezas correspondientes. Se contemplan los diseños llamados “Ball Bearing” y “Fluid Dynamic Bearing”.

Los motores tipo **BB** (“**Ball Bearing**”) por sus siglas en inglés, es decir, “Motores con Rodamientos por Balines, Balas o Baleros”. Son los primeros de su clase en ser utilizados para funcionar dentro de los DDE. Estos balines tenían constante contacto físico lo cual generaba un estrés mecánico que se traducía como vibraciones sin un patrón específico, estas tenían su origen en las imperfecciones de los rodamientos mismos. El **EPP** (“Error de Posicionamiento de Pista”) se define como aquel desfase máximo entre la cabeza y la pista deseada a leer producido por oscilaciones mecánicas; para este motor, el EEP se encontraba en el rango de las 0.1 micro-pulgadas.

Los motores tipo **FDB** (“**Fluid Dynamic Bearing**”) por sus siglas en inglés, es decir, “Motores de Rodamientos Lubricados”; son aquellos que sustituyen a los del tipo BB y son aquellos que se implementan hoy en día. Si bien estos dispositivos utilizan de igual forma rodamientos, también se caracteriza por contar con una sustancia de alta viscosidad en ellos la cual permite otorgar menor resistencia mecánica al reducir la fricción entre el motor y los balines, además, la misma viscosidad del material (típicamente aceite) absorbe las vibraciones existentes y proporciona una alta confiabilidad para los procedimientos de lectura y escritura de información, con ello, es factible entonces incrementar las RPM y reducir los tiempos de acceso a la misma. Para este motor, el EEP se encuentra en el rango de las 0.01 micro-pulgadas [4, 11].

PLATOS

También conocidos como “discos rígidos”, como ya ha sido mencionado, es dentro de estos elementos que la información es guardada en forma de señales magnéticas, las cabezas reaccionan físicamente según la tarea que se esté desempeñando con la superficie recubierta con cobalto. Para efectuar la maniobra de escritura (enviar un pulso eléctrico para generar una componente magnética), o bien, de lectura (recibir la componente magnética y transformarla nuevamente a señal eléctrica); sea cual sea la actividad ocurrente en ambos casos las señales deben de transformarse a señales digitales para poder ser interpretadas.

Estos elementos se encuentran fijos al motor mediante el uso de “abrazaderas”, fundamentalmente estas soportan la fuerza centrífuga generada por el movimiento circular del motor manteniendo una uniformidad en la densidad de bits, es decir, la velocidad angular está en función de la longitud del plato, si esta aumenta entonces la velocidad externa es mayor a la velocidad interna y se debe de ajustar la capacidad del actuador para localizar la pista deseada y sincronizar entonces el cabezal para escribir o leer según corresponda.

El diseño y estructura del plato rígido permite que este pueda almacenar información en ambas caras o solamente en una de ellas, para cada caso, el actuador deberá ser diseñado para contener una o un par de cabezas, una por cada lado para el último caso.

La información se guarda en forma de bits, los cuales son la unidad mínima de información admitida por estos dispositivos, en espacios de tamaño inferior al micrómetro; estas regiones magnéticas, en el año 2006, contaban con un tamaño estándar de 200 a 250 nanómetros radiales al plato y de 25 hasta 30 nanómetros en el sentido del giro, en total se establecía con una capacidad de 100 GB (“Giga Bytes”) por pulgada en su superficie [54]; estas regiones magnéticas son definidas durante el proceso de recubrimiento para formar “granulaciones”; esto es, este no es realizado de manera uniforme sobre la superficie ya que debido a la naturaleza de la carga magnética existirían zonas que se anularían a causa su orientación magnética en los polos mediante la generación de picos; al distribuir la capa en forma de granulaciones y al tener un tamaño y forma reducidos, su dominio magnético es lo suficientemente pequeño como para no contrarrestar a otros campos que igualmente

serían reducidos; estas granulaciones, al ser unidades independientes, no formarán picos que cancelen mutuamente otros tipos de granulaciones adyacentes en sus diferentes direcciones [54].

FABRICACIÓN

Como se mencionó anteriormente, estos se encuentran hechos de cristal, aluminio o materiales cerámicos. Ahora bien, el proceso de fabricación y deposición al vacío de capas está definido por el método conocido como “pulverización catódica” la cual consiste en la vaporización de átomos de un material base, conocido como “material blanco” a través del sometimiento a fuerzas de momento producidas por el impacto de iones energéticos, como resultado se obtiene una fina película magnética que recubre al plato [9].

El plato, después de ser sometido al procedimiento anterior, es capaz de almacenar datos de forma efectiva, sin embargo, dado que la posición del cabezal con la superficie del mismo es sensiblemente cercana (orden de los 3 nanómetros como mínimo), se necesita implementar una capa protectora que reduzca el desgaste por contacto magnético pero que al mismo tiempo permita efectuar sus operaciones de trabajo sin interrupciones al enviar y recibir señales; para ello, se implementa una capa basada en un compuesto de carbono, esta prolongará la vida útil del plato sin corrupción en la información almacenada.

En la figura 7 y tabla 10 se muestran, respectivamente, una toma paralela a la superficie del disco rígido; es importante destacar que en el espacio adyacente al establecido para que sea introducido el motor existe una zona que no está en uso y, por lo tanto, no existe información almacenada, esta zona permite colocar de forma segura el juego de cabezas del DDE cuando se encuentra en reposo.

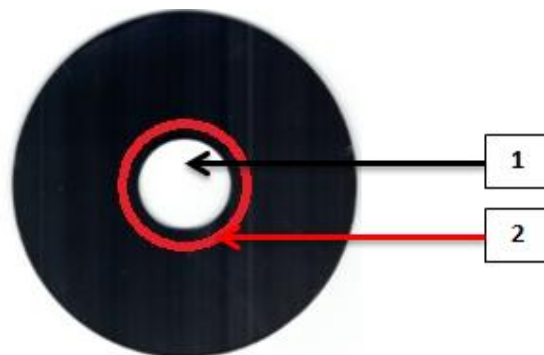


Figura 7. Plato magnetizable interno de un DDE

NÚMERO	DESCRIPCIÓN
1	ESPACIO PARA INSERCIÓN DEL MOTOR.
2	SECCIÓN ADYACENTE.

Tabla 10. Elementos constitutivos del plato magnético.

La integridad física de los platos es el factor definitivo para establecer una calidad en la información que se encuentre almacenada, así pues, si existen ciertas imperfecciones que no alteren mecánicamente al DDE pero que están claramente en decremento de la información; estas serán consideradas para definir al plato entero (al menos alguna de sus superficies) como inaccesible y/o de acceso restringido.

DISPOSITIVO ACTUADOR

Este es el componente cuya importancia es dramática en los procedimientos de extracción e introducción de datos debido a que es el encargado de establecer la comunicación directa (en ambas vías) entre la información existente en los platos magnéticos (básicamente la AS y la AU) con la interfaz de reconocimiento BIOS y el SO instalado en el DDE mediante la interacción de fuerzas electromagnéticas entre campos fijos y móviles.

El actuador completo, independientemente del fabricante, se encuentra conformado por los siguientes elementos, los cuales se explicarán a continuación:

- DISPOSITIVO VCM.
- CIRCUITO PREAMPLIFICADOR.
- CABLE PLANO DE DATOS.
- BRAZO.
- DESLIZADOR.
- CABEZAS.

El actuador es un sistema físico conjunto que provee de soporte mecánico y dinámico al igual que alimentación eléctrica hacia su elemento más importante, las cabezas; esto lo hace

durante las etapas de inicio, trabajo continuo y apagado del DDE, si bien su control físico es a partir de señales digitales provenientes de CI, su naturaleza es analógica ya que es a partir de la interacción de campos magnéticos, es decir, el generado (campo permanente) por la presencia de un par de magnetos de neodimio [84] y el generado por la bobina principal (campo transitorio) en la base que el brazo puede posicionarse en la ubicación (sector) deseada.

El dispositivo actuador establece esta relación con los platos magnéticos a partir de la utilización de las cabezas para ejecutar las instrucciones de lectura y escritura de bits, es decir, la unidad básica y mínima de valores lógicos, tales que van desde 0 a 1 según corresponda para el contenido almacenado pero siempre siguiendo la lógica positiva.

Los valores lógicos son obtenidos a partir de la relación entre la corriente incidente en la bobina de lectura/escritura y el campo magnético generado que es directamente proporcional.

Dependiendo del acoplo (dirección) diseñado por el fabricante, será como el campo producido incidirá sobre la superficie magnética en el plato, es decir, la forma en la que enviará y recibirá la información, dependiendo de la tecnología del DDE y el arreglo físico de la construcción utilizado se puede clasificar a los procesos de grabado magnético como aparece a continuación:

- GRABADO PARALELO.
- GRABADO ORTOGONAL.

Para conceptualizar las diferencias entre los tipos de grabado magnético es necesario plantear primeramente el término “**densidad de bits**”, el cual, se define como la cantidad de bits que existen por unidad de área, ahora bien, si esta densidad se considera como el doble para aquellos platos que permiten almacenar información en ambas caras, entonces se expresa una alta eficiencia en la distribución de datos.

Un aspecto determinante para obtener una eficiente densidad de bits es el factor de la temperatura, pues, la concentración de cierta energía en un espacio reducido provocará como consecuencia una componente que se convertirá en energía calorífica; si este índice

de temperatura supera cierto valor entonces el campo magnético se anulará (esto sucede cuando los dominios, es decir, las acumulaciones de cargas eléctricas orientadas en una misma dirección, pierden sus propiedades y se ven forzados a acomodarse en un nuevo orden que disminuye la fuerza magnética del conjunto) provocando con ello que el orden magnético de los platos sea aleatorio y, por lo tanto, la información almacenada será considerada como corrupta e ilegible. Atendiendo el parámetro de la temperatura y aprovechamiento del espacio mencionados, a continuación, se plantean los siguientes tipos de grabado en el plato magnético:

GRABADO PARALELO

Tal y como su nombre lo expresa, este tipo de tecnología orienta las cabezas de tal forma que no exista un grado de inclinación entre estas con respecto a la superficie en el plato. Las cargas de la magnetización producidas se inducen en el plato horizontalmente, (internamente, en cada espacio granulado en el plato los polos de la carga siguen dirigiéndose de Sur (S) a Norte (N) pero, como se mencionó anteriormente, su intensidad no es lo suficientemente fuerte como para afectar a sus homólogos adyacentes) en la figura 8 y la tabla 11 es posible visualizar el orden que siguen las cargas (bits almacenados):

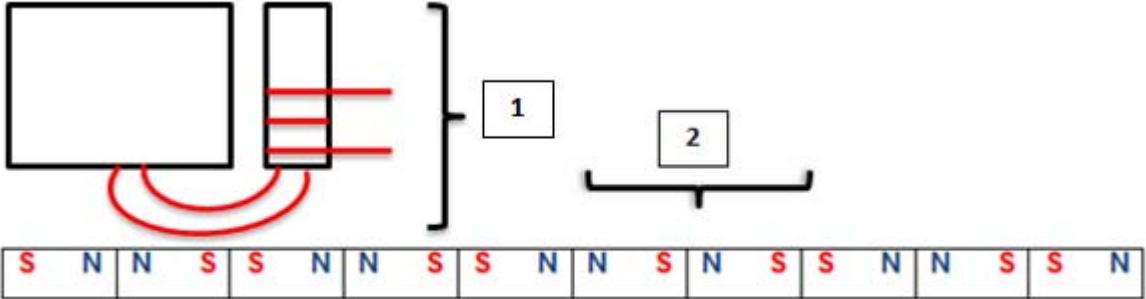


Figura 8. Grabado paralelo de datos.

GRABADO ORTOGONAL

Esta es la tecnología que predomina en la actualidad, con respecto al plano horizontal que representa el plato, las cabezas se encuentran formando un ángulo recto y las cargas son almacenadas de forma vertical. Si bien esta tecnología permite tener una mayor cantidad de bits almacenados por unidad de área, el DDE, debe de contar entonces con un plato de mayor grosor y con bobinas más potentes que atraviesen las capas hasta llegar a la zona adecuada. La distribución vertical aprovecha el flujo magnético de las cabezas ofreciendo menor resistencia a partir de la introducción de una capa extra colocada justo debajo de la superficie real de escritura y lectura, dicha capa intensifica el campo y permite con ello un menor índice de temperatura que es inversamente proporcional al gradiente de escritura. Los materiales del plato son previamente saturados y, al aplicar un cierto campo (campo proveniente de las cabezas) este puede magnetizar y desmagnetizar con mucho menor oposición (coercitividad magnética) y, por lo tanto, habrá menor temperatura resultante; es allí en donde radica su eficiencia primordial.

A continuación, en la figura 9 y tabla 11 es posible visualizar su composición.

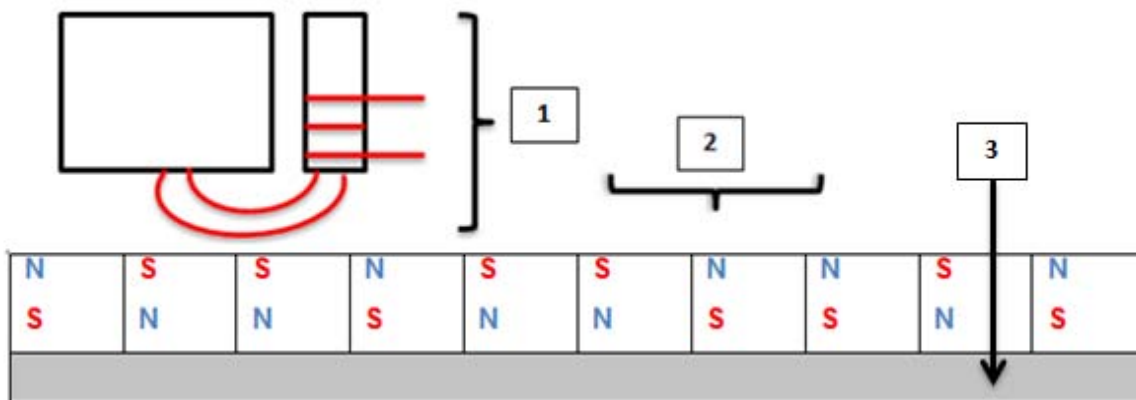


Figura 9. Grabado ortogonal de datos.

GRABADO MAGNÉTICO		
TIPO	NÚMERO	DESCRIPCIÓN
PARALELO.	1	CABEZA DE LECTURA/ESCRITURA.
	2	SUPERFICIE DEL PLATO.
ORTOGONAL.	1	CABEZA DE LECTURA/ESCRITURA.
	2	SUPERFICIE DEL PLATO.
	3	CAPA DE INTENSIFICACIÓN DE CAMPO MAGNÉTICO.

Tabla 11. Estructura física de los tipos de grabado magnético.

Dado que la temperatura no es directamente proporcional a la masa del cuerpo que la posee, el plato del DDE, teóricamente, con este arreglo puede alcanzar una densidad de bits de 155 GB por cada centímetro cuadrado superando la que se tiene con el arreglo de grabado en paralelo con 31 GB por cada centímetro cuadrado [65].

CABEZAS

Este dispositivo se define como aquella unidad física básica y mínima con la capacidad analógica de transferir y recibir señales magnéticas hacia y desde un medio magnetizable en función de un algoritmo de programación diseñado a partir de un modelo de control digital.

Actualmente, la tecnología del DDE está siendo orientada no solamente a la capacidad de almacenamiento, sino también a la capacidad de acceso a dicho espacio, por ello, se implementan un par de cabezas que rodean cada cara del plato. En el módulo *firmware* se establecen las zonas de operación para cada una de ellas reduciendo los tiempos de acceso y distancias de desplazamiento radiales en el recorrido del plato al permitir que estas codifiquen datos específicos provenientes de cada una de estas caras.

La maniobra de lectura y escritura es lograda cuando las cabezas se desplazan paralelamente sobre la superficie magnetizable del plato, sin embargo, la distancia

permanente en periodos de trabajo no existe en un momento inicial cuando el motor comienza a trabajar, así pues, la instrucción del controlador VCM es no permitir la energización de la bobina principal del actuador hasta que el motor no alcance su velocidad máxima, las cabezas se mantiene en una zona de estacionamiento lejos de la superficie de contacto; creado el flujo correcto entonces el cabezal es sostenido por una película de aire constante en toda la superficie posible de contacto; el cabezal mismo entonces se desplaza para iniciar el código de reconocimiento y carga de la información respectiva. El flujo de aire es logrado en conjunto por la carcasa, cubierta, motor y espaciadores, por ello es que la intromisión de alguna impureza podría dañar a las cabezas mismas y/o en consecuencia al plato produciendo una pérdida de información inmediata y permanente por contacto físico entre dichos elementos.

De forma específica, la cabeza recibe una corriente de alimentación proveniente de la TCI y a través del actuador; esta corriente (al pasar por el bobinado) genera un campo magnético, dado que la posición de la cabeza es paralela al plato también lo es el sentido del flujo de la corriente, la componente magnética se produce de forma ortogonal a través de un núcleo toroidal ferromagnético sobre el cual se traslada. El flujo magnético encuentra una salida en un espacio llamado “brecha” directamente hacia la superficie magnetizable y concretamente hacia el espacio designado por el mapa de bits guardado en el módulo *firmware* [4].

A continuación, en la figura 10 y tabla 12 se observan, respectivamente, un acercamiento realizado al cabezal (cabeza y deslizador conjuntos) para un DDE modelo ST-251 así como la descripción de sus elementos.

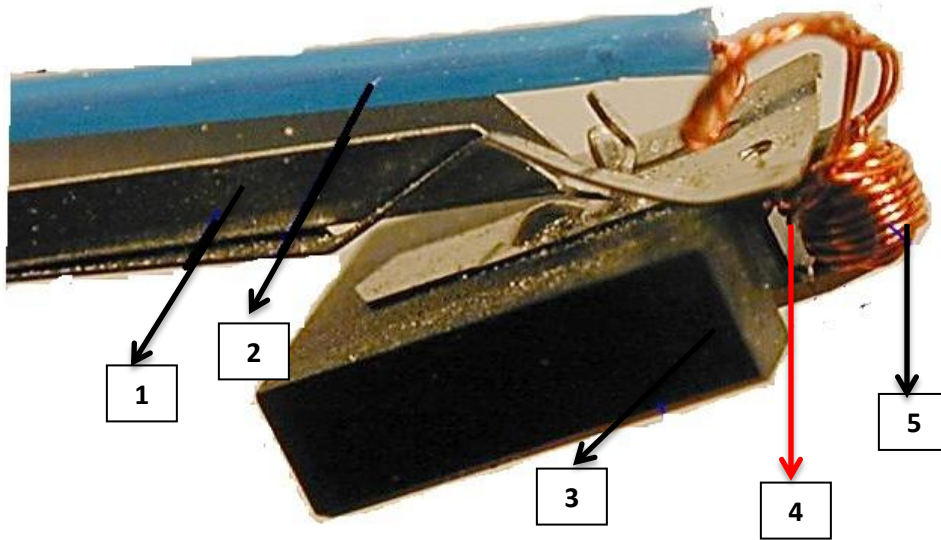


Figura 10. Acercamiento en el cabezal para un DDE modelo ST-251. Tomado de: [44].

NÚMERO	DESCRIPCIÓN
1	BRAZO.
2	FUENTE DE ALIMENTACIÓN ELÉCTRICA.
3	DESLIZADOR.
4	BRECHA.
5	CABEZA (BOBINADO).

Tabla 12. Identificación de los elementos constitutivos del cabezal.

CLASIFICACIÓN

Estos componentes pueden ser organizados de acuerdo al siguiente criterio:

1. CABEZAS DE ESCRITURA.
2. CABEZAS DE LECTURA.

Debe de especificarse que esta clasificación no es definitiva, esto es, debido a que este es el elemento más sensible y, por lo tanto, es aquel que más modificaciones sufre según se aumenten, tanto la capacidad de almacenamiento en el DDE como su velocidad y tiempos de acceso mínimos.

CABEZAS DE ESCRITURA

Estos dispositivos, mediante la utilización de un bobinado y una corriente incidente en el mismo, permiten la generación de un campo magnético que reacciona con la superficie del plato (igualmente magnético) especificando un tipo de polarización correspondiente para un valor lógico (0 ó 1). La corriente circulante por el bobinado puede cambiar su dirección e imprimir un valor lógico diferente, la programación alojada en el módulo *firmware* establece que para cada sector no pueden existir dos valores lógicos diferentes en un mismo tiempo, esta tecnología asegura que los bits guardados en la superficie no puedan ser alterados de forma accidental, intencional o errática tanto por parte del usuario como por el sistema mismo.

La naturaleza y comportamiento eléctrico y magnético de la cabeza de escritura puede ser descrito por las “Leyes de Faraday”, “Lenz” y “Maxwell” [10] [31]; las cuales establecen que: **“el voltaje inducido en un circuito cerrado es directamente proporcional a la velocidad con la que el flujo magnético es variable en el tiempo”**, puesto que el flujo magnético es variable del tiempo se expresa en forma de derivada la cual se asume como una razón de cambio; dado que la cabeza se encuentra estructurada por múltiples espiras la ecuación queda como:

$$V_l = -N \frac{\delta\phi}{\delta t} \dots (1)$$

De la ecuación (1), sus elementos se definen como:

V_I = Voltaje inducido. N = Número de espiras. $\frac{\delta\phi}{\delta t}$ = Flujo magnético variable en el tiempo.

CABEZA DE LECTURA

Al igual que las cabezas de escritura, estos elementos funcionan a partir de la relación entre campos eléctricos y magnéticos, sin embargo, para este tipo en específico (y por medio de la brecha), es que se capta la componente magnética alojada en el sector leído y se transforma para obtener su componente eléctrica que, a partir de un modelado digital, generará el valor lógico para el cual fue grabado inicialmente.

Los valores interpretados por el sistema cuando realiza los procedimientos de lectura y escritura son puramente aproximados, es a través de una etapa de electrónica digital y otra de amplificación de señales que se obtiene un valor certero, contemplado y tolerado dentro de un criterio de estabilidad.

Los dispositivos físicos que se utilizan (principalmente amplificadores y filtros para el ruido) para generar valores digitales en analógicos y a su vez analógicos en digitales se encuentran dispuestos en la circuitería de la TCI y en el circuito preamplificador, el cual, se encuentra asido al costado del cabezal.

Estos elementos adquieren sus propiedades en función de las dimensiones físicas, materiales y arreglos del módulo *firmware*. En cuanto al aspecto físico, sus dimensiones están diseñadas de acuerdo a los patrones de aire, velocidad angular del motor y factor de forma [52, 53].

En la actualidad, la tecnología predominante, en cuanto a las cabezas de lectura, es la del tipo **MRG** (“Magneto-Resistencia-Gigante”), las cuales se caracterizan por contener un par de superficies metálicas, una con acoplo fijo (solamente puede orientarse magnéticamente en una sola dirección) y la otra con acoplo múltiple (su orientación magnética depende del campo que se le aplique) divididas por un cuerpo metálico no magnético. En función de esta resistencia magnética, es que se pueden generar los valores de componente analógica

deseados; es decir, al tener una superficie en una sola dirección, la energía que se utiliza para generar su correspondiente valor es relativamente baja; ahora bien, para forzar un cambio en la dirección contraria se necesita exactamente el mismo potencial que sature a la superficie fija y la obligue a cambiar su orientación, lo cual derivará en un cambio en la componente a la salida. Para que dicha implementación sea posible, esta tecnología debe de permitir variar la resistencia magnética según se necesite de acuerdo a la influencia de un campo magnético externo (en este caso, el producido por el flujo de corriente en las cabezas). Mediante la intrusión de este campo externo la resistencia interna de la capa de intercambio decae súbitamente y permite una relativamente sencilla emisión de la componente deseada. Este procedimiento permite contener en un mismo cuerpo dos variaciones (sentidos) de una misma manifestación física de energía (magnetismo) con una alta eficiencia con respecto a la superficie de los platos.

La tecnología de MRG permite las siguientes ventajas de diseño [36]:

- Admite una densidad de área igual a 10.8 GB por cada pulgada cuadrada.
- Mejora la fluidez con la que se intercambia la excitación magnética en la superficie de los platos.
- Un DDE puede mantener su misma capacidad de almacenamiento con un menor número de cabezas y/o aumentar dicha capacidad en una misma área.

DESLIZADOR

Este dispositivo se define como aquella unidad de soporte físico y de diseño aerodinámico tal que permite sostener a las cabezas durante los períodos de trabajo prolongado permitiendo otorgar una estabilidad consistente cuando el motor de eje central se encuentra impulsando a los platos en los procedimientos de lectura y escritura de información.

El diseño del deslizador está basado en el principio que define al “trabajo”, es decir, aquella magnitud física definida como la cantidad de fuerza aplicada por una distancia establecida, es decir:

$$T = (F)(S) \dots(2)$$

De la ecuación (2), sus elementos se definen como:

$T =$ Trabajo.

$F =$ Fuerza.

$S =$ Distancia.

Al ser una relación directamente proporcional, la distancia que se recorre desde el punto de contacto de la bobina principal (distancia inicial) hasta su extremo superior (distancia final) del deslizador son diferentes y con ellos también lo son las fuerzas actuantes en estos. La fuerza que se transmite a través del brazo y hasta el deslizador, al igual que su velocidad de desplazamiento, son mayores y, por ello, es que este dispositivo no puede contener una gran masa ante un repentino cambio en la energización y/o en la posición del brazo mismo que produjera fricción por contacto físico que inmediatamente incendiara la cabeza produciendo la destrucción de esta y de la información contenida en los platos.

Como ya se ha mencionado a lo largo del presente trabajo de investigación, la presencia de impurezas, contaminantes y/o fisuras en la superficie de los platos se traduce inmediatamente como una corrupción del medio físico y la consecuente destrucción de los datos allí contenidos, por ello es que este ambiente no admite alguno de estos cuerpos que le comprometan.

Existen etapas en las que la velocidad del motor no es constante, estas son durante la fase de energización y la de desenergización. Si bien se estableció que el dispositivo actuador no comienza sus movimientos sino hasta que el motor de eje central haya alcanzado su velocidad en RMP máxima, esto no sucede cuando se suprime el suministro de energía de forma súbita (falla en la alimentación), con ello el patrón de aire cambia y existe una diferencia de presiones internas, por lo tanto, existe riesgo de contacto físico; esto se soluciona mediante un diseño a base de surcos dispuesto en el deslizador (figura 13), los cuales brindan una sobre-suspensión momentánea suficiente que permita al brazo colocar a las cabezas nuevamente en su posición de descanso (figura 11) y/o en su área de estacionamiento en una rampa (figura 12) sin que estos cuerpos logren entrar en contacto el uno con el otro de forma efectiva.

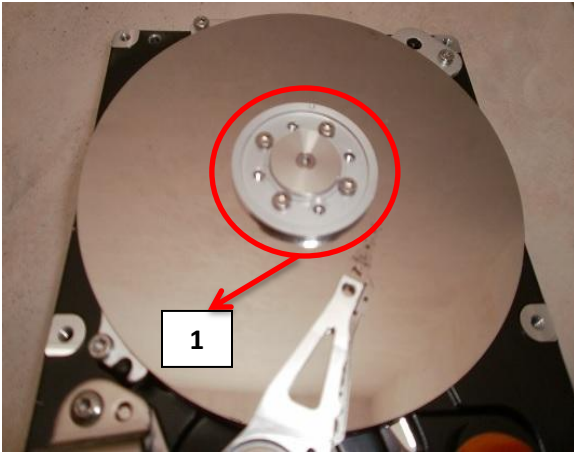


Figura 11. Cabezas en zona de estacionamiento (1).

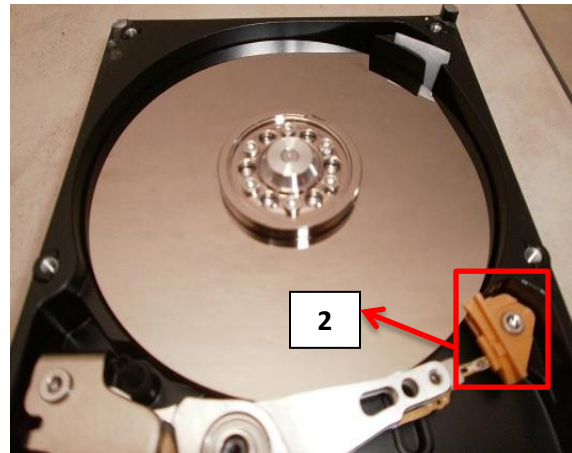


Figura 12. Cabezas en la zona de estacionamiento (2).

En las figuras 11 y 12, respectivamente, es posible visualizar el par diferente de arreglos que existen para situar a las cabezas cuando se encuentran en estado de reposo. Para el caso del primero, el círculo rojo indica que toda aquella zona que no puede ser ocupada por información, dicha instrucción de restricción se encuentra almacenada en el AS del módulo *firmware* guardado en la memoria ROM de la TCI.

Para el caso del segundo arreglo, se observa que la totalidad del plato se encuentra libre del dispositivo actuador y este último se posiciona en un espacio conocido como “zona de arranque y/o zona de estacionamiento aislada” la cual, mediante el acoplamiento de una rampa, permite al brazo expandirse verticalmente separando las cabezas y evitando cualquier posible contacto entre estas.

Actualmente, la tecnología de acoplo por rampa es la que se mantiene vigente debido a sus altos estándares de seguridad de operación; mismos cuales, contemplan las siguientes medidas:

1. Ante la presencia de una falla eléctrica, corrige el error producido en el actuador en el que este se golpeaba ante la base del motor cuando se suprimía su alimentación.
2. Ante un estado de reposo (desconexión total), corrige el error producido cuando el DDE sufría una caída, aunque los platos no se encontrasen girando estos sufrían un impacto consistente en contra del bazo actuador de forma longitudinal destruyendo múltiples zonas de almacenamiento de datos.

A continuación, se muestra un acercamiento realizado a un dispositivo deslizador de un DDE; al igual que la descripción de sus elementos en la tabla 13, respectivamente.

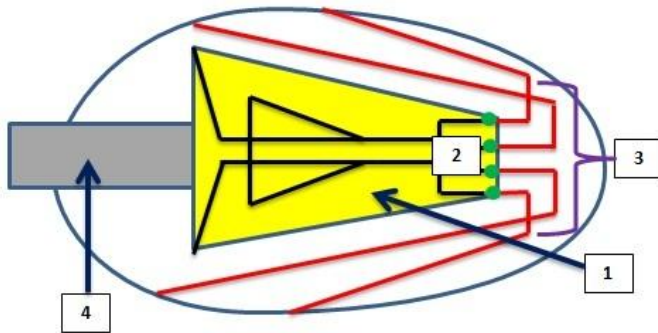


Figura 13. Distribución física del deslizador (diagrama).

NÚMERO	DESCRIPCIÓN
1	DESLIZADOR.
2	CABEZA.
3	LÍNEAS DE ALIMENTACIÓN.
4	BRAZO.

Tabla 13. Elementos constitutivos del deslizador.

El arreglo a base de surcos mencionado anteriormente introduce un nuevo concepto en medidas de seguridad, pues, es diseñado específicamente para generar una “película de aire fluido” que se define como un colchón de aire auto-regulado que aprovecha el ímpetu remanente del motor para suspender de forma temporal al deslizador y así posicionarlo en sus respectivas zonas de estacionamiento [45].

BRAZO

Se define así a aquella estructura metálica que contiene a los dispositivos involucrados en el proceso de inserción, extracción e interpretación de señales analógico-digitales (cabezas y circuito preamplificador) y, también como aquel que soporta el estrés físico proveniente de los movimientos oscilatorios y vibratorios producidos por las fuerzas de interacción magnéticas en el VCM.

El brazo se encuentra construido de aluminio, esto es debido a que este material es capaz de soportar con rigidez las vibraciones sin verse alterado su factor de forma y, a su vez, lo suficientemente ligero como para responder ante los movimientos indicados por el campo magnético generados en la bobina principal del actuador.

La humedad es un factor que expone al aluminio la presencia de moléculas de oxígeno que tienden a oxidarle, sin embargo, este último tiene la propiedad de sólo reaccionar con este

metaloide en su superficie inmediata y no así en su núcleo, por lo que la estructura no pierde rigidez y resistencia ante el estrés mecánico aplicado. [72]

A continuación, en la figura 14, se observa un cabezal desmontado de la carcasa para un DDE modelo WD800AAJS.



Figura 14. Brazo, cable plano de datos y bobina principal para un DDE.

De la imagen anterior, debe de mencionarse que este modelo de DDE específicamente sólo cuenta con una cabeza de lectura y escritura asida al brazo, esto significa que sólo una de las caras del plato magnético contiene la totalidad de la información almacenada.

CABLE PLANO DE DATOS

También conocido como “bus de datos”, este dispositivo permite la comunicación directa entre las cabezas y el circuito preamplificador de forma bidireccional; su diseño permite filtrar el ruido producido durante las etapas de operación del DDE tanto para las señales analógicas como digitales.

La razón de que exista un cable de datos en un espacio tan reducido se justifica por la intensidad de las señales producidas tanto en las cabezas como en el preamplificador, esta debe de ser lo suficientemente alta como para transmitirse de un punto a otro, pero no tanto que permita la producción de señales de ruido hacia los circuitos de control.

Los materiales de construcción de este elemento son una base plástica aislante en la cual se encuentran contenidas las pistas de material semiconductor asidas a los extremos de los dispositivos interconectados, es decir, en los puertos de entrada/salida del circuito preamplificador así como en los contactos de las cabezas dispuestas en la cara anterior del deslizador. En los primeros modelos se podían encontrar puntos de contacto a base de oro,

esto debido a su apreciable conductividad, posteriormente se emigró a un sistema base de plata que permitía niveles aceptables de la misma sin corrosión aparente, actualmente los diseños están enfocados a base de aluminio y cobre.

En la figura 14, es posible visualizar que la forma en la que se adapta el cable de datos es flexible, dicha propiedad debe de permanecer a fin de evitar fracturas internas en las pistas y/o rigidez que limite el movimiento libre del brazo. Dicha condición impediría la correcta lectura y escritura de valores en los platos magnetizables y generaría una resistencia mecánica que intentase compensarse en forma de una sobre-corriente en la bobina principal del actuador, por lo que los procesos de lectura y escritura no sólo se verían afectados y comprometidos, sino también el tiempo de vida útil del alambre magneto.

CIRCUITO PREAMPLIFICADOR

Se define como aquel circuito de comunicación eléctrico-electrónico, control e interpretación de datos inmediato al arreglo de cabeza/cabezas en el DDE. Es un microcontrolador del tipo encapsulado que se encarga del posicionamiento del actuador mediante la interpretación de señales provenientes desde y hacia este mediante la utilización del sistema CCS. El cable plano de datos es elemento físico de interconexión a través de cual, el circuito preamplificador, recibe y envía señales. A continuación, en las figuras 15 y 16, se muestran, respectivamente, los estados dinámicos de funcionamiento posibles para el elemento descrito.

Funcionamiento durante el estado de escritura

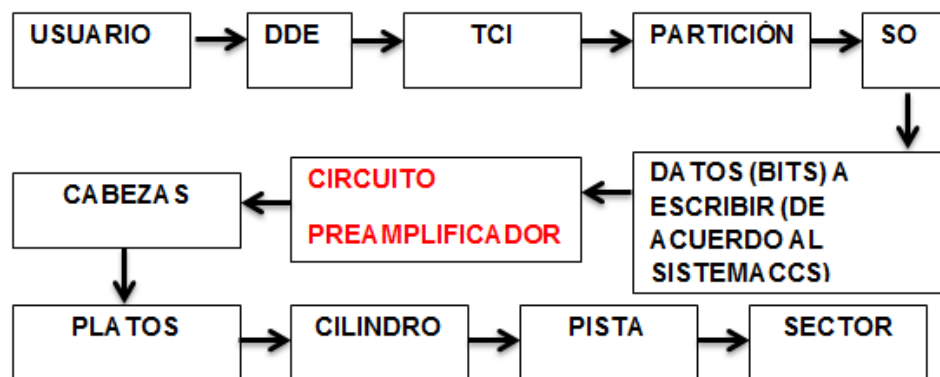


Figura 15. Comportamiento del circuito preamplificador durante la escritura de datos.

Funcionamiento durante el estado de lectura:

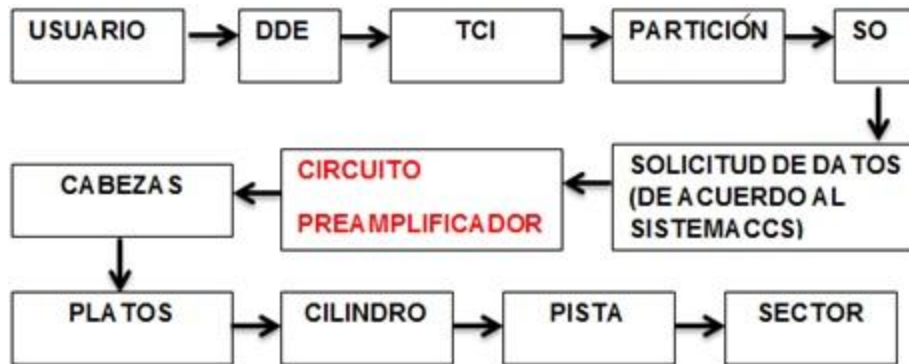


Figura 16. Comportamiento del circuito preamplificador durante la lectura de datos.

El funcionamiento de los buses de entrada/salida (estados) no ocurre en tiempos idénticos, es decir, se dice que sólo son multiplexados en espacio y, mientras que uno se encuentre activo el otro se mantendrá pasivo hasta que la instrucción de operación de cambio de estados solicite lo contrario. En adición, toda operación de escritura y lectura de datos conlleva una etapa de filtrado y modulación de señales para minimizar y/o anular el error a la entrada o salida del sistema analógico-digital.

Básicamente, los puertos de entrada y salida de datos tienen una configuración que les evita estar activos en mismos tiempos, el espacio de envío de información puede ser compartido, dicha característica es propia de los sistemas de comunicación serial.

Habiéndose establecido el conjunto de elementos físicos básicos del DDE; es necesario entonces plantear aquellos otros elementos virtuales que realizan las dinámicas de control y que, en la práctica, representan aquellos valores lógicos (información) apreciable a fin de ser recuperados cuando existe algún tipo de corrupción que comprometa su integridad.

1.3.2 ESTRUCTURA LÓGICA

Este tipo de estructura se define como aquel arreglo virtual de *software* programable contenido es un medio físico que esquematiza, distribuye, organiza, interpreta y ejecuta instrucciones de operación bajo un orden basado en un modelo digital de almacenamiento de datos.

Esencialmente, la estructura lógica corresponde a todo el conjunto y jerarquización de operaciones virtuales (diseño lógico) de los espacios asignados para el almacenamiento de datos en los platos magnetizables.

En esta sección se analizará el arreglo que las unidades de DDE deben seguir para obtener la característica de escribir datos y, a su vez, leerlos nuevamente; así como los tiempos y pulsos pertinentes. En la tabla 14 se pueden observar el conjunto de unidades de almacenamiento (encontrados y definidos en el mapa de memoria del módulo *firmware*) que existen contenidos en el DDE basados en una lógica binaria.

ESTRUCTURA LÓGICA	
UNIDAD	DEFINICIÓN
BIT (b).	Unidad mínima y básica de información en sistemas digitales, puede adquirir solamente valores de 1 y 0 que indican la presencia y ausencia, respectivamente de datos que obedecen a la lógica positiva [55].
BYTE (B).	Unidad básica de información significativa de un sistema digital. Se encuentra conformado por una cadena ordenada de 8 bits [55]. De igual forma, esta cantidad de bits es la mínima para que un sistema computacional pueda expresar un carácter (letra, número, dígito y/o símbolo) [74].
SECTOR.	Unidad mínima de datos significativos accesible por las cabezas del DDE, dependiendo del tipo de formato establecido este puede ser de 512 bytes para DDE y de 2048 bytes para discos ópticos. Igualmente, se define como aquella área comprendida

	entre un par de zonas limítrofes adyacentes de diferente diámetro.
PISTA.	Es un anillo radial, concéntrico y/o cadena de sectores consecutivos asignados dentro del mapa de memoria del módulo <i>firmware</i> con tiempos y velocidades de acceso específicos e idénticos.
ZONA.	Conjunto de pistas adyacentes con diferentes frecuencias y, por lo tanto, diferentes tiempos de acceso, basado el modelo Bits Por Pulgada (BPP), una zona externa al centro del plato tendrá una mayor frecuencia que una zona interna [78].
CLÚSTER.	Denominación que, de acuerdo al tipo de “Sistema de Archivos” (SA), se refiere a la cantidad de sectores contiguos necesarios para almacenar información. Dependiendo de la extensión y/o tamaño de la información almacenada, esta puede colocarse en diferentes clústers sobre los cuales se encuentra asignado el inicio y fin del archivo mismo.
CILINDRO.	Arreglo tridimensional vertical de pistas de diferentes platos que comparten el mismo tiempo de acceso [4].

Tabla 14. Organización jerárquica de la estructura lógica en el DDE.

La información almacenada en el DDE está definida por instrucciones de acceso, dichas instrucciones le indican a las cabezas tanto la ubicación como los tiempos (pulsos) que se deben de contemplar a fin de acceder a un sector específico cuando el usuario y/o SA lo soliciten para las operaciones de escritura y lectura de datos, según corresponda.

Existen un par de métodos, también conocidos como “identificadores”, que estos dispositivos utilizan a fin de ubicar los sectores, pistas y cilindros correspondientes, es decir, los datos e información del usuario así como la del SO instalado. A continuación se coloca su descripción.

SISTEMA DE IDENTIFICACIÓN CCS

Consiste en la identificación **CCS** (“Cabeza, Cilindro y Sector”) en el cual, se ha almacenado la información a partir del enrutamiento por bloques. Dentro del mapa de memoria de la TCI el DDE se identifica una dirección preestablecida y asignada para cada uno de los sectores, luego se localiza la cabeza a la cual corresponde dicho sector y finalmente el cilindro adecuado; posteriormente, el actuador se posicionará en la dirección indicada. Es de suma importancia identificar todo el cilindro pues debido a que la información puede estar contenida en una o varias pistas, el cilindro siempre deberá de ser accesible a fin de no tener solamente ciertas piezas de la información. En un modelo ideal, después de una corrupción física o lógica de los elementos encargados de la lectura y escritura de datos, toda la información estará almacenada e íntegra siempre y cuando exista una perfecta alineación vertical del cilindro (dicha alineación vertical se establece desde la fabricación de los platos magnetizables) y no exista daño de las superficies (caras) del mismo.

La tecnología CCS fue implementada en aquellos arreglos de DDE que fueron iguales o menores a 8 GB como capacidad máxima de almacenamiento; la razón por la cual este sistema no se extiende para capacidades superiores es por el estrés el memoria y recursos que esto exige, lo cual lo volvería preciso pero ineficaz en términos de aprovechamiento de energía, es decir, totalmente obsoleto dado que para cambiar de sector tendría que recurrir una y otra vez al mapa de memoria, comparar la dirección encontrada con la mapeada y finalmente leerla, o bien, escribirla [1, 2, 78].

Sin embargo, el sistema CCS se utiliza actualmente como la forma principal de acceso a bajo nivel en DDE, esto brinda la utilidad de identificar, evaluar y diagnosticar sectores en específico y la información contenidos en ellos.

SISTEMA DE IDENTIFICACIÓN DBL

Este método consiste en la asignación automática y única de un código numérico para cada sector; esta asignación comienza desde el 0 hasta el sector final, es decir, depende del tamaño y/o longitud del disco. El término **DBL** (“Dirección de Bloque Lógico”) es comúnmente interpretado como sinónimo para referirse a un sector, sin embargo esto no es precisamente correcto. La longitud de un sector (como ya se ha especificado previamente) para un DDE es de 512 bytes los cuales coinciden con la extensión de un tipo de DBL, sin embargo podría darse el caso que el sector tuviese una extensión de 1024 Bytes y su DBL también; por ello es que antes de definir su extensión, hay que identificar cuál ha sido el tamaño del sector asignado de acuerdo al SA incorporado.

Para los fines del presente proyecto de investigación solamente se estudiarán los SA del tipo **NTFS** y **FAT32**, estos acrónimos significan, respectivamente, lo siguiente: (“**New Technology File System**”), es decir, “Nueva Tecnología de Sistema de Archivos” y, (“**File Allocation Table**”), es decir, “Tabla de Asignación de Archivos”, (ver páginas 56, 57 y 58, respectivamente) [57, 58].

Como un ejemplo práctico, considérese un DDE con una capacidad de 500 GB identificados en sus datos de placa, considerando un SA de tipo NTFS el valor correspondiente para cada sector sería de 512 bytes, por lo tanto, el respectivo DBL calculado e identificado seguiría la siguiente ecuación:

$$DBL = \frac{\Phi}{\Upsilon} \dots (3) \text{ , de la ecuación anterior sus argumentos se definen como:}$$

DBL = Sectores totales del DDE.

Φ = Capacidad (datos de placa).

Υ = Bytes de cada sector.

Sustituyendo valores en la ecuación (2).

$$DBL = \frac{500GB}{512B} \dots (3') \quad DBL = 976562.50 \text{ sectores.}$$

El resultado anterior significa que el DDE tendrá una asignación que comienza desde el número 0 hasta el valor de 976562, el término decimal se elimina, pues, no pueden existir fracciones de sectores.

El DBL es definido a partir de un método llamado “servo-sectores” desde el momento de la fabricación, el cual es un proceso de seccionamiento magnético; sus ubicaciones se almacenan en el módulo *firmware* y la UMC puede recurrir a estas localidades de forma predeterminada sin identificar previamente el cilindro y cabeza correspondiente. Este procedimiento agiliza significativamente los tiempos de acceso y respuesta que se necesitan para procesar los distintos tipos de información almacenados.

Debido a la distribución circular de las pistas y sectores por diseño, se ha establecido tener una mayor concentración de sectores en las pistas exteriores que en aquellas interiores; esta práctica ayuda a equilibrar la cantidad de información posible a ser accedida con aquella que realmente puede ser obtenida, a este método específico de grabación se le conoce como “grabado de bit por zona” [8].

En la figura 17 siguiente, se visualiza la distribución de los elementos conformantes de la estructura lógica, nótese que el concepto de “cilindro” sólo es aplicable cuando se tienen solamente un par y/o más platos dentro de la carcasa y la alineación entre estos será esencial.

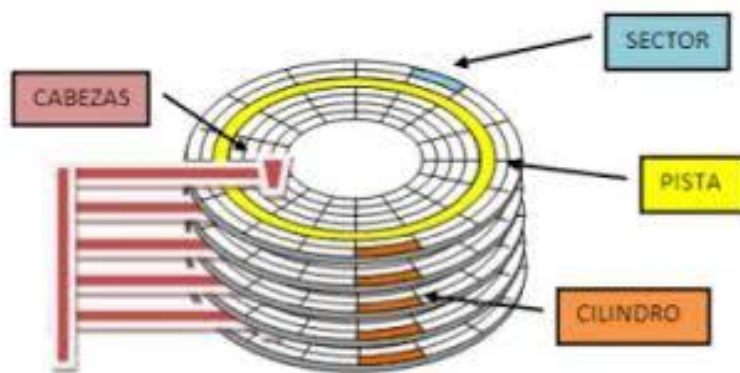


Figura 17. Distribución y arreglo lógico dentro del DDE Tomado de: [26].

De la figura anterior, se comprueba que los cilindros se encuentran definidos en función del número de pistas totales que los platos sean capaces de contener y, que la cantidad de sectores por pista y cilindro es inversamente proporcional a la distancia medida desde el centro del motor de eje central hasta al borde exterior del plato magnetizable.

Tanto los circuitos de control digital almacenados dentro (circuito preamplificador) y fuera de la carcasa (arreglo de TCI) como los elementos descritos anteriormente, están regidos por tiempos y definiciones específicas de operación que, en conjunto, permiten ejecutar comandos para acceder a la estructura lógica del DDE y, por lo tanto, a la información allí contenida. A continuación, se mencionan y clasifican dichos elementos [4 78, 35]:

CARACTERÍSTICA DE TIEMPOS

Tiempo de lectura y escritura: magnitud de tiempo suficiente que el DDE emplea ya sea para leer o escribir información en un sector o sectores, a su vez, este es dependiente de la cantidad de datos solicitados, cantidad de bloques utilizados, velocidad y número de las cabezas, así como la cantidad de sectores por cada pista.

Tiempo medio de búsqueda: magnitud de tiempo suficiente para colocar la cabeza en la pista correcta.

Tiempo completo de búsqueda: magnitud de tiempo total que se define como aquella necesaria para que el cabezal encuentre la pista y regrese a su posición inicial de reposo, o bien, hacia la siguiente pista a acceder.

Latencia: magnitud de tiempo de retraso intencional dada entre el posicionamiento del cabezal sobre la pista y el sector solicitados, este desfase se aplica debido a que en el instante mismo que el actuador posiciona la (s) cabeza (s) no es posible ejecutar las instrucciones de lectura/escritura.

CARACTERÍSTICA DE PISTAS

Densidad de pista: se refiere a la cantidad de pistas concéntricas que existen por unidad de área basado en un sistema de coordenadas cilíndricas.

Bloque de pista: compone el conjunto de bits secuenciales y pistas consecutivas adyacentes.

Búsqueda de pista: se refiere al tiempo mínimo necesario y posible en el cual la cabeza cambia su posición de una pista hacia otra.

Seguimiento de pista: se refiere a la compensación forzada utilizada para posicionar el cabezal en el centro de la pista y minimizar el estado de error lo más posible a fin de mantenerlo dentro de un sistema estable.

CARACTERÍSTICA DE DENSIDADES

Densidad de bits: mencionado anteriormente, se refiere a la cantidad de bits almacenados por unidad de área cuadrada comprendidos por una sola pista, se contabilizan bajo el sistema BPP.

Densidad de pista: se refiere a la cantidad de pistas que existen por unidad de área cuadrada comprendidos de forma paralela al plato, se contabilizan bajo el sistema **PPP** (“Pistas Por Pulgada”)

CARACTERÍSTICA DE VELOCIDAD

Memoria Cache: Arreglo de memoria tipo RAM cuya función es la de agilizar el proceso de lectura/escritura al guardar las direcciones previamente accedidas y otorgarlas cuando el actuador completo deba de posicionarse nuevamente en estas.

El código establecido por la tecnología DBL en cada uno de los sectores está considerado para evitar fallos tales en los que la información fuese sobre-escrita, es decir, cada localidad con información guardará justo al inicio del sector un indicador, también llamado “bandera” que muestra que se encuentra ocupado, de esa forma la cabeza recibe dicha información y se procederá a buscar la siguiente localidad más inmediata cuyo indicador muestre un estado disponible [100].

El DDE, como se ha citado previamente, es sistema de información basado en señales analógicas, digitales y con un SO asociado, ahora bien, previo a este SO, existe un SA tal que permite presentar, dividir y sincronizar distintos elementos externos e internos al

mismo DDE; este conjunto de elementos se encuentran categorizados y conforman una arreglo estratificado y siempre secuencial, dicho arreglo se analizará a continuación.

ORGANIZACIÓN LÓGICA

Para abordar el estudio de esta sección, en la tabla 15, se muestra la división a seguir, la cual, indica los componentes lógicos que permiten la correcta visualización, interpretación y presentación de la información.

ELEMENTOS CONSTITUTIVOS		
FORMATO PRIMARIO	FORMATO SECUNDARIO	ÁREA DE ALMACENAMIENTO DE DATOS (AAD)
<ul style="list-style-type: none"> • FORMATO PROFUNDO. 	<ul style="list-style-type: none"> • FORMATO SUPERFICIAL. 	<ul style="list-style-type: none"> • SECTOR RAP (REGISTRO DE ARRANQUE PRINCIPAL).
<ul style="list-style-type: none"> • Características de operación. 	<ul style="list-style-type: none"> • Características de operación. 	<ul style="list-style-type: none"> • PARTICIONES.
		<ul style="list-style-type: none"> • TIPO DE SA.
		<ul style="list-style-type: none"> • SECTOR RISO (“REGISTRO DE INICIO DE SISTEMA OPERATIVO”).
		<ul style="list-style-type: none"> • AMBIENTE DEL SO.

Tabla 15. Elementos constitutivos de la organización lógica del DDE.

De la tabla anterior, se establece que existen diferentes de tipos de formato; esto debido a que el DDE, para que pueda ser utilizado formalmente, necesita generar e identificar los diferentes sectores, pistas y cilindros a partir de entradas y salidas de bytes basados en las áreas de almacenamiento de datos anteriores. Estas áreas permiten, metodológicamente, la entrada y salida de información [100]. A continuación, los elementos expuestos en la tabla 15 son explicados y definidos.

FORMATO PRIMARIO

Este término hace referencia a la generación de todas aquellas condiciones lógicas tales que permitan la identificación del DDE justo como un sistema de almacenamiento de datos y no

solamente como un conjunto mecánico de elementos controlados por señales digitales a base de *software*.

Cuando existe una corrupción en esta fase lógica, esencialmente el DDE es totalmente inservible puesto que se carece de la capacidad de tener acceso a este, de manipular la información y/o de interactuar con cualquier otro sistema, incluido el *software* BIOS.

A su vez, el formato profundo conforma el aspecto medular del formato primario ya que establece dichas condiciones lógicas añadiendo una interfaz de datos.

FORMATO PROFUNDO

Proceso de asignación, creación y división física en sectores, clústers, pistas, zonas y cilindros de la superficie del plato magnetizable. Este tipo de formato interviene directamente los platos y establece el patrón a seguir de acuerdo a cada configuración diseñada por los fabricantes; es decir, que no todos los procedimientos de formato profundo aplican para un DDE de una marca específica.

Características de operación:

1. Permite realizar pruebas de estrés físico (lectura/escritura) sobre la superficie del plato.
2. Identifica los sectores cuyos tiempo de respuesta comienzan a extenderse y que, potencialmente, podrían dañarse y comprometer la información contenida en ellos.
3. Segmentación y distribución de las pistas concéntricas.
4. Establecimiento del arreglo de sectores específicos para cada pista y sus intervalos de operación (tiempos de acceso).
5. Establecer los identificadores de cada sector (“banderas”) y los asocia a cada pista generada.
6. Cuando un identificador se encuentra ilegible, corrupto y/o dañado realiza un intento por direccionarlo lógicamente en otra localidad pero, de no ser posible, intentará entonces eliminarlo del mapa de acceso predeterminado en el módulo *firmware*.

FORMATO SECUNDARIO

Para presentar la definición de este método de formato es necesario mostrar antes las definiciones y diferencias fundamentales en cuanto a lo que respectan los discos físicos y los discos lógicos; los cuales, se muestran a continuación:

Disco físico. Se refiere al dispositivo real de almacenamiento, es decir, el *hardware* que es conectado por medio de interfaces y circuitos, asociado e identificado por un sistema computacional mediante un arreglo de *software* BIOS y, subsecuentemente, por un SO [87] mediante una interfaz de conexión (figura 18) [71].



Figura 18. Unidad de *hardware* completa para un DDE.

Disco lógico. También conocido como “volumen”, se refiere al dispositivo/interfaz virtual a la cual, mediante el uso de programas y aplicaciones, se le asigna un SA y una letra del alfabeto bajo un ambiente de SO.

El disco lógico permite la interacción del usuario con su información, esta a su vez se encuentra contenida en espacios asignados por un SA llamados “particiones” [8] las cuales básicamente son divisiones lógicas interactivas que existen en una superficie física real (platos magnéticos) y son controladas, administradas, configuradas y modificadas a través de un *software* y, en las cuales, se alberga un SO [64].

Es posible establecer que que todo el conjunto de configuraciones, modificaciones y manipulaciones de la información tiene lugar en los volúmenes/particiones de un DDE, por lo tanto, tanto el *hardware* como el *software* son directamente dependientes.

Para el caso del disco lógico, en la figura 19, se considera un entorno básico de *software* tipo MS-DOS [17], es decir, un SO de bajo consumo de recursos cuya interacción es a través de líneas de comandos y establecimiento de argumentos/parámetros de operación. Para este en particular, tanto el volumen como su respectivo SA del DDE han asignado la letra “C” para la partición seleccionada.

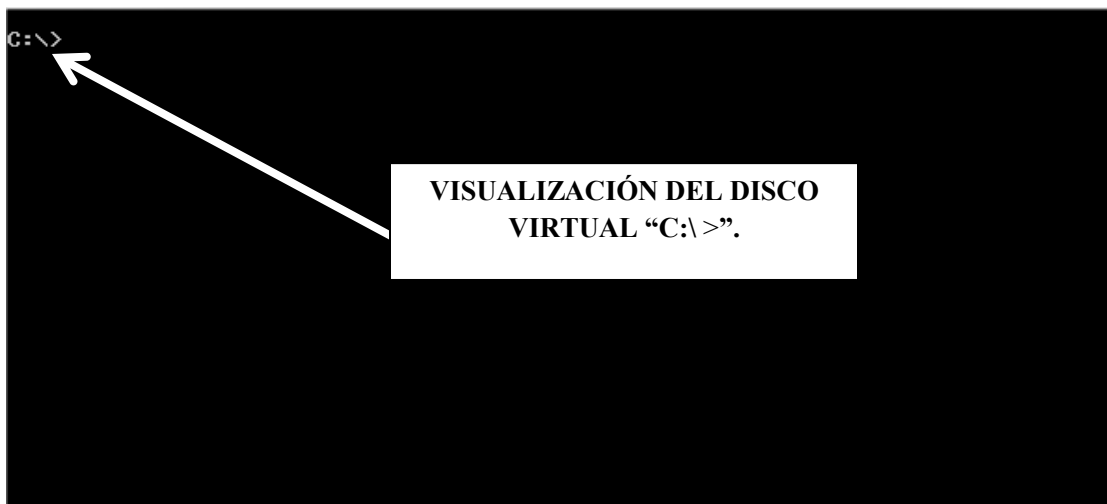


Figura 19. Visualización en entorno MS-DOS de un disco lógico identificado como “C:”.

Una vez establecidas los conceptos anteriores, el **formato secundario** se define aquella capacidad específica de un *software* para, dentro de una unidad de *hardware*, establecer, configurar, administrar, interpretar, interactuar, informar, direccionar y relacionar el conjunto de elementos virtuales con los elementos físicos disponibles; así como la característica misma de generar locaciones (directorios a partir de un SA) en los cuales se organiza y jerarquiza la información del usuario y del SO instalado [100].

A diferencia del formato primario, el formato secundario es universal y no depende de la marca asociada al DDE, sólo depende, básicamente, de la interfaz física de conexión y el SO asociado.

Los volúmenes/particiones y/o discos lógicos están gobernados fundamentalmente por un elemento llamado sector RAP, este sector funge como la entrada principal para la ejecución

de todos los anteriores y, este a su vez, se ubica dentro del área de almacenamiento de datos, la cual se describe a continuación.

ÁREA DE ALMACENAMIENTO DE DATOS

Comprende todas aquellas direcciones (también llamadas “localidades”) posibles y accesibles que comprenden el AS y el AU, es decir, una localidad puede almacenar información que, por motivos de seguridad y de integridad de la unidad misma, el usuario promedio no puede manipular y que bajo un ambiente de SO no le es visible. Considérese como ejemplo el área de *firmware* que se encuentra almacenada en los platos magnéticos; ahora bien, se dice que es accesible porque se necesita utilizar equipo e instrumentos especializados para acceder de forma correcta, segura y eficiente.

Matemáticamente, el AAD (“Área de Almacenamiento de Datos”) totales se encuentra descrita por la siguiente ecuación:

$$AAD=AS+AU \dots (4)$$

En resumen, el AS se encuentra protegida de ser accedida por el usuario mediante una tecnología que evita mostrar dichas localidades, en tanto que el AU es perfectamente manipulable por este de forma directa.

SECTOR RAP

También conocido como “sector cero”. Es el primer sector físico existente en un sistema de almacenamiento de datos; para el caso del DDE, su ubicación (utilizando el sistema CCS) es la localidad: cabeza 0, cilindro 0 y sector 1. El sector RAP conforma en sí mismo una estructura de datos tal que permite el reconocimiento físico y lógico del DDE ante el *software* BIOS.

Características de operación:

1. Al momento de energizar el sistema computacional, el sector RAP le permite al *software* BIOS leer su contenido para así este último tomar el control y cargar el contenido de la tabla de particiones y el SO instalado en ella.
2. Contiene la información (en lenguaje máquina) sobre los tipos y características de cada una de las particiones del DDE, de esa manera el BIOS detectará aquellas marcadas aptas para contener un SO o solamente información del usuario, para el caso en que se existan ambos tipos de particiones, el BIOS privilegiará la del SO.
3. Concede el control al sector de inicio de cada partición activa una vez que se ha comprobado la integridad de la misma, de lo contrario buscará la siguiente y de no existir, regresará un valor en pantalla para indicar que ninguna partición cumple con los requerimientos. Realizando las acciones anteriores se garantiza que no existan daños por lectura a la información almacenada.
4. Contiene un último elemento de seguridad (el cual puede ser opcional) incorporado, “**la firma de disco**”, tiene una extensión de 32 bits que identifican sin posibilidad de fallo el tipo de *hardware* conectado. El BIOS identificará aquellas unidades que no sean un DDE y procederá o no a discriminarlas de su proceso base de lectura de información de inicio.

A continuación, en la tabla 16, se muestra la composición lógica del sector RAP. Nótese que, como cualquiera de los sectores expuesto en la presente investigación, tiene un tamaño de 512 bytes [15, 100].

ELEMENTO	DESCRIPCIÓN
CONTENIDO DE LA TABLA DE PARTICIONES.	64 bytes.
CÓDIGO MÁQUINA DE GESTIÓN DE ARRANQUE.	446 bytes.
FIRMA DE UNIDAD (INDICA SI CONTIENE O NO UNA PARTICIÓN ACTIVA).	2 bytes.

Tabla 16. Estructura lógica del sector RAP.

De la tabla anterior, en el apartado de “tabla de particiones”, nótese que la extensión de 64B admite hasta 4 entradas de particiones de 16B cada una.

La información del usuario y la del SO se almacenan, en teoría, en diferentes tipos de particiones, cada una con diferentes características y propiedades. A continuación se presentan sus definiciones y clasificaciones para cada caso.

PARTICIONES

Su definición ha sido mostrada anteriormente, sin embargo esta puede ser estudiada desde el punto de vista organizacional de la información y adquiere entonces un nuevo significado. Estas secciones del DDE, en su registro principal (los identificadores inmediatos) le indican al sector RAP si contiene información del usuario o si solamente contiene un SO en ellas, así como su tamaño y ubicación; independientemente del SA asociado a la partición existen una clasificación general dada de acuerdo a su función.

Para los fines de la presente exposición, solamente las particiones primarias y secundarias serán analizadas.

TIPOS DE PARTICIONES

Partición primaria: aquella porción del dispositivo de almacenamiento de datos generada a partir de la implementación de un SA; puede ser identificada y utilizada por un SO y, de la misma forma, a la cual se le puede asignar una dirección lógica (volumen definido por una letra del alfabeto) para contener la instalación lógica de un SO.

Partición secundaria: aquella porción del dispositivo de almacenamiento de datos diseñada para contener unidades lógicas. El sector RAP (como se mencionó anteriormente) tiene una capacidad de hasta 4 particiones; entonces y en un intento de superar dicho impedimento, la partición lógica albergará volúmenes basados en un SA indirecto [15].

TABLA DE PARTICIONES

Este es el contenido más apreciable del sector RAP, consta de un grupo de 64B dividido en 4 particiones sobre las cuales se indican [16]:

1. Tipo de partición (de inicio o de datos).
2. Estado de la partición (activa o inactiva)
3. De acuerdo al sistema de identificación CCS, el sector inicial y sector final de la partición.
4. De acuerdo al sistema de identificación DBL, tamaño total de la partición (sectores).
5. Tamaño de cada partición y/o sectores empleados por estas.

En la figura 20, se plasma la división física que compone exclusivamente la tabla de particiones del sector RAP.

1 byte .	3 bytes .	1 byte .	3 bytes .	4 bytes .	4 bytes .
TIPO DE PARTICIÓN .	CCS INICIAL .	TIPO DE PARTICIÓN .	CCS FINAL .	TAMAÑO TOTAL DE LA PARTICIÓN .	SECTORES OCUPADOS POR LA PARTICIÓN .

Figura 20. Distribución, expresada en bytes, de la tabla de particiones para el sector RAP.

Es importante especificar que para el caso de la cadena de 8 bits que definen el tipo de partición, será del tipo “inicio” cuando sus primeros 7 caracteres se encuentren en 0 y el último dígito esté en 1; para el caso contrario, si todos sus dígitos encuentran marcando un 0, entonces la partición contendrá datos.

SECTOR RISO

Dicho sector, de acuerdo al sistema CCS, se ubica en cabeza: 1, cilindro: 0 y sector: 1. Este elemento es el encargado de recibir una señal (proveniente del sector RAP) para poder comenzar la descarga y lectura de código de aquella partición activa que contenga un SO, por lo tanto, el sector RAP es forzado a ceder el control pero sigue manteniéndose habilitado, pues, en el reside la tabla de particiones que, de forma permanente, el sector RISO leerá cada que se realice un apagado e inicio del SO [22].

Características de operación:

1. Este sector es el primero en ser leído por el SO.
2. Contiene un *software* definido como: **PBBIOS** (“Parámetros de Bloque del *software* BIOS”) [25], el cual, se encarga de identificar y analizar las propiedades

físicas y lógicas del DDE tales como aquellos espacios con partición y sin partición y, para el caso de los espacios particionados, describe el volumen asignado a esta.

SISTEMA DE ARCHIVOS

Se puede definir como aquel conjunto de instrucciones automatizadas con una lógica de programación tal que permite a los sectores (y las particiones que estos conforman) establecer patrones de lectura y escritura de datos bajo un entorno de organización de los mismo por medio de directorios, carpetas y ubicaciones específicas en memoria, todas estas, controladas por un SO.

Características de operación:

1. Administración y uso de memorias periféricas.
2. Visualización, asignación, y ubicación del espacio libre y espacio ocupado por archivos del SO (incluidos los del usuario).
3. Presentan una estructura de forma textual y/o gráfica organizacional de la información perteneciente a la unidad de almacenamiento de datos.
4. Relaciona la ubicación de la información de acuerdo a los sectores que esta ocupa, de esa manera, cuando el usuario decida acceder a la información, el SA concede a su vez el acceso a dichas ubicaciones. Inicialmente el archivo deberá de estar en sectores consecutivos, sin embargo y con el uso diario del SA, los archivos (en sectores) tienden a dividirse lo que genera un incremento visible en los tiempos de acceso de datos.
5. De la misma forma que en el punto anterior, el SA ubica de forma eficiente aquellos sectores disponibles y aquellos que potencialmente podrían ser utilizados.

De forma general, el SA provee la capacidad de crear, diseñar, abrir, redireccionar y eliminar archivos y/o directorios en su totalidad.

Citado anteriormente, existen diferentes tipos de archivo con diferentes distribuciones y arreglos de la información, sin embargo las características previamente mencionadas son generales y aplicables a estos. Para el estudio de los diferentes tipos de SA, en el presente proyecto de investigación, sólo serán contemplados los sistemas NTFS y FAT32 [51].

SISTEMA NTFS

Denominado como “Sistema de Archivos de Nueva Tecnología”. Es un SA típicamente utilizado por sistemas base Windows [99] para sus versiones liberadas a partir del año 2002.

En este SA se contempla una estructura denominada como **TMA** (“Tabla Maestra de Archivos”). Es la encargada de contener a detalle la información, características y propiedades físicas (sectores e identificadores) y lógicas (ubicación) de la información contenida en la tabla de particiones. Por motivos evidentes de seguridad, la estructura TMA no puede ser accesible por el usuario.

La localización de información (archivos) se realiza a través de un arreglo binario ramificado, de esa forma, la identificación de sectores y datos contenidos conlleva un menor tiempo puesto que la búsqueda se realiza de forma múltiple en vez de solicitudes y respuestas individuales.

El SA NTFS contempla una directiva de seguridad en la que ningún proceso (ejecutado o no por el usuario de forma directa o indirecta) puede tener influencia sobre algún archivo sin antes haber comprobado sus credenciales (es decir, todo el conjunto de permisos y atributos de propiedad que un usuario puede poseer sobre un archivo) ante los módulos de acceso del SO asociado.

Contiene un sector único al inicio de su estructura denominado “sector de inicio” el cual funge como un desencadenador de código y, esencialmente, de este depende la carga del SO. Si este sector recibe la información de reconocimiento del *software* BIOS, la identificación del *hardware* y, en adición, los demás elementos de inicio propios del SO; entonces este último procede a ejecutarse [61, 99, 100].

Características de operación:

1. Teóricamente, el SA NTFS puede alcanzar una capacidad de almacenamiento de 17000 mil millones de TB; sin embargo, el modelo real sugiere que, hasta el momento, sólo es alcanzable la capacidad de 8TB (DDE modelo “Seagate Archive”).

2. Implementa la tecnología de permisos, cifrados y restricciones de alta complejidad utilizados para la protección de elementos lógicos sensibles.
3. Brinda la opción de “auto-compresión” para los archivos contenidos en el volumen, con esta característica, se puede ahorrar espacio de almacenamiento sin comprometer la disponibilidad del elemento comprimido. La compresión se realiza al modificar el tamaño virtual de un sector, en tanto que el sector físico sigue manteniendo un valor de 512B.
4. Implementa la tecnología llamada “*Journalising*” (la cual se activa ante un evento de cerrado y/o apagado inesperado) que consiste en la ejecución de una instrucción de auto-reparación basada en la última consulta estructurada, válida y funcional antes del apagado súbito. Esta tecnología ejecuta dicha línea de comando y, finalmente, establece una la posible restauración.

En la figura 21 se visualiza el arreglo lógico del SA NTFS, así mismo, nótese que esta tecnología permite separar de forma eficiente la entrada (o bien diferentes entradas) a la información crítica de la información misma del SO y el usuario; de esa forma, si existiera algún fallo en estas la información sería inaccesible pero potencialmente recuperable.

1 byte .	3 bytes .	1 byte .	3 bytes .	4 bytes .	4 bytes .
TIPO DE PARTICIÓN .	CCS INICIAL .	TIPO DE PARTICIÓN .	CCS FINAL .	TAMAÑO TOTAL DE LA PARTICIÓN .	SECTORES OCUPADOS POR LA PARTICIÓN .

Figura 21. Estructura interna para el SA tipo NTFS.

Composición estructural de la TMA

Esta implementación exclusiva del SA NTFS está dirigida a centralizar las características de los datos contenidos en un sólo espacio para poder obtener, manipular y agilizar los tiempos de acceso a la ubicación real de la información. Los elementos integradores de la TMA se describen a continuación:

Decriptor. Módulo que permite conceder o negar privilegios de acceso y propiedad de datos para cada archivo identificado. Ante una falla por corrupción de lectura en este módulo, el SA NTFS dispone una copia del mismo.

Registro de eventos. Módulo que proporciona información sobre el conjunto de acciones, modificaciones, accesos y fechas efectuados a la zona de datos (partición), la cual, incluye tanto al SO como archivos diseñados por el usuario.

Núcleo. Módulo de control en donde se guardan los atributos de los bloques (conjuntos ordenados por categoría y jerarquía de varios tipos de archivos y sus directorios); de esta forma, cada elementos con su respectivo directorio tendrá un registro propio en la TMA.

SISTEMA FAT32

Denominado como “Tabla de Asignación de Archivos”, este SA de 32 bits, al igual que el NTFS, funciona a partir de la asignación de entradas a directorios que contienen la información, así pues, se compone de estructuras en donde se almacenan los datos y características de los archivos contenidos [14].

La primera estructura es denominada como “directorio principal” y es la encargada de asimilar las direcciones (sistema DBL), nombres de los archivos, tipos de extensiones, tamaños y utilización de sectores que cada uno de los directorios ocupados. De forma complementaria, los contenidos reales (información de alta prioridad por el usuario y el SO) y los directorios son colocados a manera de clústers que tienden a ser consecutivos.

Los procedimientos de identificación de la información se llevan a cabo en una segunda estructura denominada como “**FAT**”, la cual, está diseñada para coordinar todo el conjunto de sectores y clústers utilizados. Anteriormente se mencionó que estos tienden a ser consecutivos, sin embargo cuando se realiza una eliminación de datos estos son propensos a colocar remanentes y piezas de información corrupta en sus entradas y ocasionan que cada vez una mayor cantidad de sectores sean ocupados y estos pertenezcan a diferentes localidades; la consecuencia lógica de estas operaciones reiteradas es que los tiempos de ubicación, de acceso, de solicitud de apertura y de sincronización con el entorno gráfico proporcionado por el SO sean cada vez mayores. El aumento en tiempos no sólo minará la eficiencia del SA sino que acelerará el proceso de deterioro físico de las cabezas al realizar maniobras exhaustivas de lectura y escritura, a esto se le debe de añadir el desgaste físico que de igual manera sufre el actuador completo.

El SA FAT32 contempla una copia de seguridad inactiva de la FAT llamada FAT 2 que se encuentra adyacente a la primera, esta es una copia con los parámetros de operación iniciales y una instrucción le indicará que se active si es que la actual en uso sufre algún daño.

El SA FAT32 cuenta con una tercera estructura llamada “sector de arranque” el cual puede ser el equivalente del sector RISO en el SA NTFS ya que es el primer sector lógico para cada una de las particiones. Este sector leerá el contenido guardado en el sector RAP, encontrará la tabla de particiones activa que contenga el SO y lo ejecutará manteniendo a las demás particiones identificadas como “activas” pero de datos, a su vez, la tabla de particiones contendrá un campo, el cual ejecuta una instrucción de identificación única, esta última debe de informar que se trata de una estructura tipo FAT32 no corrupta.

A continuación, en la tabla 17 se presenta una descripción detallada de los componentes estructurales de la FAT.

ESTRUCTURA	DESCRIPCIÓN
SECTOR DE ARRANQUE.	Presenta ante el <i>software</i> BIOS la información que define las características lógicas tales como el tipo de disco lógico, tipos de archivo y el código desencadenador que ejecuta al SO.
SECTORES RESERVADOS.	Conjunto de sectores excluidos de los procesos normales de lectura durante la operación de la partición, se utilizan para controlar a la FAT y la FAT 2
FAT.	Estructura que contiene medularmente todo el conjunto de datos, información, directorios, direcciones lógicas y estados de asignación para los “clústers” utilizados.
FAT 2.	Bloque de datos inactivo que contiene una

	copia legible de la estructura FAT original, constituye una tecnología de seguridad e integridad del SA.
DIRECTORIO PRINCIPAL.	Contiene información detallada y altamente descriptiva sobre los archivos y folders únicos de la raíz de la partición.
ZONA DE DATOS.	Contiene todo el conjunto de valores lógicos, archivos e información sobre el SA y el SO.

Tabla 17. Estructura lógica de la zona FAT en el SA FAT32.

Básicamente, este sistema funciona con un par de áreas, la “zona FAT” y la “zona de datos”. Todo el contenido de la zona FAT indica características y protocolos de lectura de instrucciones para la ejecución de procesos de control antes, durante y después de un SO activo, en tanto que la zona de datos se encarga de mantener la información medular del volumen.

Para un SA FAT32 el término “clústers”, presentado en la tabla 14, adquiere una nueva acepción, es decir, aquí representará todo aquel espacio mínimo asignable utilizado para contener algún dato completo, de esa forma un clúster puede dejar de ser un conjunto de sectores para pasar a ser uno del tamaño de 512B. Aquellos clústers que sean válidos serán detectados y enumerados desde el inicio de la partición inmediatamente después de realizar los procedimientos de identificación del *software* BIOS.

CONCLUSIONES PARCIALES

En este capítulo se estudió al DDE como un dispositivo compuesto por un par de estructuras: mecánica y lógica. Dichas estructuras son independientes en protocolos de operación pero están interconectadas para poder ejecutar las maniobras propias de identificación, detección, operación y, principalmente, lectura y escritura de datos por medio de una relación comprendida dentro de los criterios de estabilidad a través del *software* y el *hardware*. Analizar las dinámicas de funcionamiento de ambas resultará en mejores condiciones para la delimitación de las fallas y, con ello, los procedimientos de reparación y recuperación de información pertinentes.

CAPÍTULO 2. FALLOS EN LA ESTRUCTURAS

Los elementos descritos en el capítulo anterior pueden presentar alteraciones que, de forma parcial y/o definitiva, pueden potencialmente destruir la información del usuario evitando implementar cualquier técnica de recuperación de datos existente, o bien, una muy específica.

En este apartado se describirán aquellas fallas de origen virtual (problemáticas relacionadas a la ejecución y aplicación del *software*) y físicas (relacionadas directamente al *hardware* y los espacios de información físicos de control involucrados) que pueden suceder en el DDE durante sus etapas de inicio, operación continua y reposo. Así mismo, se mencionarán las características de las mismas indicando sus consecuencias y posibles métodos de solución para cada caso.

2.1 CORRUPCIONES LÓGICAS Y POSIBLES MÉTODOS DE REPARACIÓN

Esta estructura, como se estudió en el capítulo anterior, conforma la totalidad de la información del DDE y contempla ciertos datos que, directa e indirectamente, son necesarios para poder realizar una lectura y recuperación exitosas. Existen diferentes y únicas condiciones para que se presenten fallos y/o corrupciones lógicas que inevitablemente comprometan el contenido de los disco rígidos, pues, también dependerá de la ubicación de estos (ya sea en AU o el AS) así como el SA predominante en el volumen y, en adición, la arquitectura de SO instalado.

En toda estructura lógica estudiada para almacenamiento de datos (como lo es el DDE) se ha contemplado la tecnología S.M.A.R.T. (ver página 15); la cual, ejecuta evaluaciones, medidas y predicciones de futuras fallas basadas en algoritmos de programación, estas a su vez, tienen el objetivo de proteger la información del usuario antes de que las estructuras mecánicas y lógicas colapsen completamente. Siempre que las condiciones lo permitan, es de vital importancia atender los valores del módulo S.M.A.R.T. con el fin de prevenir el realizar una recuperación en la que ya exista la posibilidad de daño físico extensivo.

Se le llama **daño lógico** a toda aquella condición de índole virtual y de *software* que impida el acceso a la información almacenada en una unidad de forma parcial y/o total por medio de la alteración de los mecanismos de lectura y escritura llevada a cabo tanto interna como externamente por los dispositivos implicados.

En esta sección se expondrán las problemáticas más comunes así como las técnicas propias para cada caso, indicando la descripción de los procesos y los resultados parciales/totales obtenidos acordes al método y/o técnica empleado.

Se mencionó anteriormente la definición para “daño lógico”, sin embargo esta puede ser extendida hasta el concepto de **fallo por *software***, el cual a su vez se define como toda aquella alteración, corrupción, error de lectura y ejecución en la dinámica de operación que acontece en un sistema de control diseñado por instrucciones lógicas, la cual, deriva directamente en la degradación de la calidad de información almacenada en una unidad digital [4, 20].

Aplicando la definición anterior al objeto de estudio analizado, un fallo por *software*, específicamente, estará presente en el DDE cuando se muestren alteraciones en la arquitectura de datos en las siguientes estructuras:

1. Módulo *firmware* (tanto el almacenado en la TCI como en los platos magnetizables).
2. Con la condición mostrada en el punto anterior, se produce una anulación del *software* BIOS para detectar al DDE conectado al sistema computacional.
3. Alteraciones en la estructura RAP.
4. Alteraciones en la tabla de particiones.
5. Corrupción del SA para NTFS y FAT32, al igual que el SO instalado en el volumen.
6. Elementos borrados, formateados y sobre-escritura de manera parcial y/o total por causa de *software* vírico.

Las condiciones anteriormente descritas pueden ser ocasionadas, fundamentalmente, por las razones siguientes [82, 100]:

1. Ataque por *software* del tipo virus informático.

2. Tipo de formato aplicado a la unidad de almacenamiento.
3. Supresión del suministro de energía eléctrica durante los momentos de carga, ejecución y/o apagado del sistema computacional.
4. Interrupción (desconexión física de la interfaz) de datos durante las etapas de lectura y escritura de datos.
5. Sectores, bloques e incluso pistas inaccesibles.
6. Condición de corto-circuito en los arreglos de CI y/o elementos directamente dependientes de estos.

Las problemáticas y respectivos métodos de solución parciales y/o totales (igualmente temporales) expuestos se implementarán a través de la utilización de *software* libre [37], así como distintas herramientas de *hardware*.

Debido a la incidencia, relevancia como casos de estudio, complejidad y procedimientos que esto representa, **para el presente proyecto de investigación**, se analizarán exclusivamente aquellos daños lógicos referentes a:

- A) CASO 1: SECTOR RAP (FIRMA “0XAA55”).
- B) CASO 2: TABLA DE PARTICIONES.
- C) **CASO REPRESENTATIVO 3: CORRUPCIÓN DEL SO A CAUSA DE INFECCIONES POR PROGRAMAS DEL TIPO “VIRUS INFORMÁTICO”.**

El inciso C) es resaltado debido a que atiende directamente al impedimento principal de la reparación lógica: la ejecución del BIOS, SO y/o plataformas lógicas de operación, pues, no es posible recuperar información de una unidad de DDE si es que esta no es reconocida previamente por los *softwares* correspondientes.

2.1.1 CASO 1: SECTOR RAP (FIRMA “0XAA55”)

Un deterioro en el código de programación interno en este sector (ya sea por condiciones de *software* como un ataque por virus, o bien, del *hardware* por degradación de la superficie magnetizable del plato) puede evitar que se descargue a su vez el micro código para iniciar el acceso a la tabla de particiones/volumen e iniciar la secuencia del SO.

Las estructuras básicas del sector RAP son: la tabla de particiones y la firma de sector “0XAA55”; dichas estructuras no deben sufrir alteraciones ya que, de lo contrario, provocarán que el sector RAP no sea leído, ejecutado e invocado de manera correcta a través del *software* BIOS.

La **firma “0XAA55”**, también conocida como “espacio de comprobación” ubicada en los bytes 511-512, es aquella encargada de proporcionar la validación del sector RAP, de tal forma que se compruebe que su valor sea el correcto para abrir el resto de los 510 bytes posibles. Esta sección contiene un valor dado en sistema hexadecimal [30] igual a “0XAA55 y/o AA55H”. Si este valor no corresponde al asignado para estos bytes, entonces el sector regresa un valor en pantalla indicando que se encuentra corrupto, dañado y/o que no existe una partición desde la cual iniciar la carga del SO.

En las figuras 22 y 23, respectivamente, se muestran los síntomas (mensajes) que un sistema computacional experimenta cuando la firma “0XAA55” ha sufrido daños en su estructura.

Los mensajes en pantalla, dependiendo de la arquitectura de SO instalado en el volumen, pueden mostrar de forma parcial cierta información y/o códigos de error para obtener asistencia técnica.

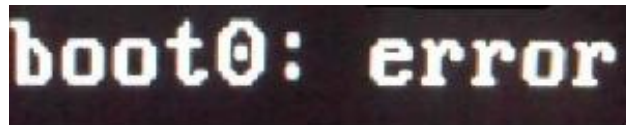


Figura 22. Visualización de mensaje de error para un fallo en la lectura en el sector de inicio.



Figura 23. Visualización de mensajes de error para fallas en la firma “0XAA55” del sector RAP (1).

Si el *software* BIOS es incapaz de validar al sector RAP entonces todo su contenido nunca se activará y este sector no podrá ceder el control al sector RISO. Lo mencionado anteriormente es, esencialmente, el problema principal cuando se presentan esta clase de alteraciones de programación, por ello, debe de existir un método para reasignar el valor correcto a la firma y se proceda con la comprobación de la misma.

Cuando acontece un fallo de esta naturaleza, el DDE no puede ser reparado de forma directa, es decir, dado que no existe un SO accesible en el volumen, ningún *software* contenido en este podrá ser ejecutado, por ello es necesario acoplarlo a un nuevo sistema computacional en el que ya exista otra unidad de DDE con un SO instalado y las herramientas necesarias.

DESCRIPCIÓN DEL PROCESO DE REPARACIÓN

Se visualiza, en la tabla 18, el DDE (figura 24) degradado en su estructura RAP con los datos de placa (y lógicos) siguientes:

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	HGST.
MODELO.	HTS545050A7E380.
DBL.	976773168 SECTORES.
INTERFAZ.	SATA.
CAPACIDAD DE ALMACENAMIENTO.	500 GB.
VOLÚMENES CONTENIDOS.	1 DISCO LÓGICO (UNIDAD "C").

Tabla 18. Datos de placa para DDE con degradación del sector RAP.

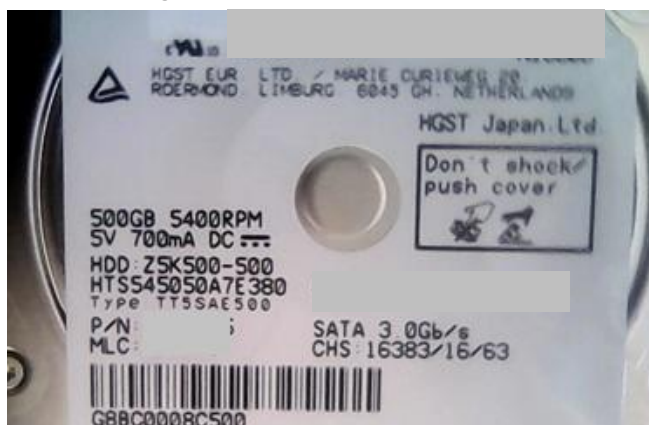


Figura 24. Visualización de datos de placa del DDE dañado por degradación en el sector RAP.

Para el caso de estudio en particular de este DDE, el origen de su daño es puramente lógico, esto debido a que sufrió un ataque por *software* tipo “virus informático” identificado como “ZAccess” [7] y, durante su etapa de desinfección, el sector RAP resultó colateralmente afectado.

PROCEDIMIENTO

De forma genérica, la reparación para este tipo de daños es, típicamente semi-automatizada y mediante la utilización de *software* de diseño, los cuales, independientemente de su creador, contemplarán las siguientes condiciones con el fin de reconstruir la arquitectura del sector RAP sin que se vean alteradas las demás estructuras internas [62]:

1. Acceder al DDE a través de una consola de recuperación externa, la cual, lo utilizará como “objetivo” en vez de “fuente” para la carga de los archivos necesarios para la reparación. Sobre dicha consola se ejecutarán todo el conjunto de comandos por *software*.
2. Ejecutar las modificaciones única y exclusivamente en la dirección CCS definida como: cabeza 0, cilindro 0 y sector 1.
3. El *software* de reparación se almacenará temporalmente en la memoria RAM instalado en el sistema computacional.
4. Se listarán todas las unidades de DDE conectadas (aunque el DDE afectado no pueda iniciar el volumen por sí solo, siempre será detectable la unidad física cuando otro sistema computacional lo invoque) en las diferentes direcciones y mostrará sus características tales como su capacidad de almacenamiento y tipo de interfaz de conexión.
5. Se deberá de seleccionar la unidad física de DDE afectada basándose en el DBL proporcionado en los datos de placa de la unidad, seleccionar otra podría significar una modificación de los valores de las particiones en un segundo DDE y provocar un daño en su respectivo sector RAP.
6. Una vez definida la unidad física, el *software* realizará un procedimiento denominado como “*by-pass*”, el cual, consiste en acceder directamente a todo el conjunto de discos lógicos contenidos en la tabla de particiones, aquí se identificará

el tipo de SA asociado al volumen y, de forma complementaria, la ubicación externa de los archivos utilizados para la restauración del sector RAP.

7. El *software*, mediante el uso de comandos de fábrica, invocará los archivos de inicio de código, aquellos que han sido corruptos y en los que se encuentra contenida la “firma 0XAA55” a fin de ser alojados en el sector deseado, de ser necesario, en cada volumen.

Llegado a este punto, el *software* tiene que realizar un par de funciones basadas en los datos que obtuvo como respuesta a la solicitud en las unidades lógicas, es decir, una vez detectadas aquellas que contengan un SO se realizarán las siguientes acciones:

1. Se actualizará el conjunto de instrucciones de código necesario para el arranque del SO, es decir, el *software* interno del sector RAP, con dicho contenido el DDE podrá iniciar de forma correcta y el sector RISO se ejecutará de forma regular.
2. Aquellos volúmenes que sean de inicio serán actualizados en todos sus sectores RAP, en tanto que aquellos volúmenes dinámicos [85] (pueden contener múltiples discos lógicos integrados por distintas unidades físicas sin que necesariamente tengan un SO instalado) se mantendrán intactos.

Dado que la consola de recuperación está alojada en una sección temporal (memoria RAM) los cambios y ejecuciones deben de consolidarse en una sola exhibición, es decir, cualquier interrupción en el procedimiento significará que las modificaciones podrían ser parciales y el problema continuaría.

Los efectos y cambios generados podrán ser visibles bajo las siguientes condiciones:

1. El DDE debe ser conectado nuevamente a la unidad computacional original a la que pertenece.
2. De ser necesario, se deberá de configurar al DDE como la unidad única con la cual el sistema computacional puede iniciarse.

Para el caso mostrado, el daño en el sector RAP, particularmente, se encontraba expresado por condiciones en las que fue corrupto desde el momento de su infección, es decir, la integridad de la información estaba comprometida debido a que este tipo de *software* no se

limita exclusivamente a esta zona reservada del AS, sino que una vez que ha logrado vulnerar el *firmware* y haber escrito su código en este sector, intentaría propagarse hasta cubrir por completo el AU, culminando así, la destrucción definitiva de la información contenida en la unidad.

Normalmente, de ser ejecutados todos los pasos anteriores, el DDE se encontrará reparado y con la información del AS y el AU intacta. A continuación, en la tabla 19 se muestra, de forma condensada, el conjunto de operaciones y de resultados obtenidos a partir de la implementación del método de reparación expuesto.

ELEMENTO	TIPO DE DAÑO/CARACTERÍSTICAS	MÉTODO APLICADO	RESULTADOS
SECTOR RAP Y FIRMA 0XAA55 CORRUPTOS.	LÓGICO, CON IMPOSIBILIDAD DEL USUARIO PARA INICIAR EL SO Y/O ACCEDER A LA INFORMACIÓN.	REPARACIÓN SEMI-AUTOMATIZADA POR COMANDOS A TRAVÉS DEL USO DE LA CONSOLA DE RECUPERACIÓN EXTERNA.	OPERACIÓN EXITOSA.

Tabla 19. Componentes del sector RAP, tipo de daño, método de reparación aplicado y resultados obtenidos.

A continuación, en las figuras 25 y 26 se visualizan, respectivamente, los estados anterior y posterior al procedimiento de reparación aplicado, nótese que aunque el DDE a reparar se encuentra detectado por el *software* “*diskmgmt.msc*” [96, 99] (figura 25) este no es accesible y se detecta como “**No asignado**”, posteriormente, mediante el uso del mismo *software* ahora se muestra un estado en donde el disco lógico es nuevamente visible y accesible por el usuario (figura 26).



Figura 25. Visualización del DDE a través del *software* “*diskmgmt.msc*” por corrupción en el sector RAP.



Figura 26. Visualización del DDE a través del *software* “diskmgmt.msc” por corrupción en el sector RAP (reparado).

CONCLUSIONES PARCIALES

En esta sección se observó el comportamiento previo y posterior a la reparación por *software* semi-automatizado de un DDE con un deterioro en la información del sector RAP, así como su respectiva visualización a través de un ambiente de SO.

En un modelo real, las condiciones de falla del sector RAP pueden ser catalogadas como: **parciales** y **definitivas**; esto es, aquellas que son parciales (como la expuesta en el presente estudio) permiten la manipulación, reparación, restauración y reprogramación de su contenido a fin de ser modificadas para regresar a valores de fábrica y permitir una eficiente extracción de la información; en tanto que las definitivas son aquellas que, sin importar el conjunto de herramientas de *software* y *hardware* utilizadas, no podrán responder a ningún método de reparación (considérese el caso en el que el sector RAP estuviese fisurado físicamente y/o deteriorado en su superficie magnética, el acceso sería totalmente restringido catalogando a este DDE como irrecuperable).

2.1.2 CASO 2: TABLA DE PARTICIONES

Se estableció en el capítulo anterior que el sector RAP puede contener hasta 4 particiones, cada una con 16B de tamaño, dando como resultado un total de 64B. Típicamente, cuando acontecen estos daños la estructura que resulta minada es la TMA completa (esta condición sólo aplica cuando la TMA es atacada por *software* malicioso tipo “virus”), entonces ninguna de las particiones será visible. Aunque con una menor incidencia, las tablas de particiones individuales también pueden verse afectadas

Se dice que existe un **daño en la partición** cuando el SO instalado en el DDE (debe de asumirse que la partición dañada no es primaria ya que no contiene al SO), a través del “explorador de archivos”, es incapaz de conceder acceso a la partición cuando exista una

solicitud por parte del usuario. Se presentan un par de síntomas inequívocos que indican la presencia de dicha condición, a continuación, se presentan aquellas más representativas:

1. El SO solicita al usuario formatear el volumen encontrado, si sólo existe uno, pedirá entonces el formateo del DDE completo.
2. El SO indica que el SA asociado al disco lógico es incompatible o está dañado.

Atendiendo los puntos anteriores, en las figuras 27 y 28 se muestran, respectivamente, las condiciones descritas con volúmenes lógicos diferentes.



Figura 27. Visualización de la solicitud del SO para formatear una tabla de particiones vulnerable.

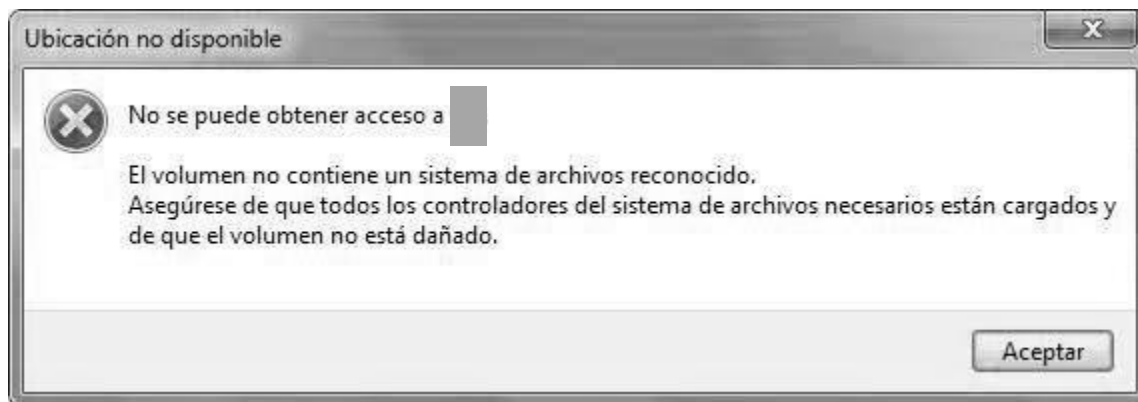


Figura 28. Visualización del mensaje de error por incompatibilidad en el SA instalado.

La recuperación, ya sea de la TMA y/o de una partición en específico, estará dividida en un par de campos, los cuales, contienen características de comportamiento únicas entre sí, las cuales se describen a continuación.

PÉRDIDA DE LA PARTICIÓN

Se le denomina así a la condición reversible en que el disco lógico se visualiza como inexistente y/o desconocido. Este fenómeno sucede cuando se alteran ciertas localidades de la tabla de particiones. A continuación, en la figura 29, se observa el conjunto de bytes que conforman a su vez el arreglo de 16 bytes único para cada partición.

BYTE DE INICIO.	CCS INICIAL.	TIPO DE PARTICIÓN.	CCS FINAL.	DBL TOTAL.	TAMAÑO.
1B	3B	1B	3B	4B	4B

Figura 29. Distribución, expresada en bytes, de la tabla de particiones.

De la figura anterior, si las localidades identificadas: bytes de inicio y tipo de partición son alteradas en su contenido (borrado y/o cambio en el valor lógico) la partición será indetectable por el sector RAP aunque la firma de comprobación se encuentre activa.

Para el caso de un ataque por *software* tipo “virus informático” [50], este siempre modificará el bit número 7 del primer byte de la partición, el cual (como se mencionó anteriormente), indica el estado de la partición, es decir, si es de inicio o de almacenamiento. Por otra parte, un *software* malicioso igualmente puede afectar el contenido del bloque identificado como “tipo de partición”, borrándolo y anulando igualmente la identificación de la misma.

A continuación, se presentan el conjunto de causas que provocan un fallo daño consistente de la partición:

1. Alteración manual y/o por *software*.
2. Supresión súbita de la alimentación eléctrica durante el periodo de operación permanente del SO instalado.
3. Procesos incompletos de copiado de particiones, a través, de la utilización de *software* especializados.
4. Borrado intencional del disco lógico.
5. Utilización de *softwares* como “*diskmgmt.msc*” para la modificación, ampliación, reducción y unión de uno o varios volúmenes.

DAÑO CONSISTENTE EN LA PARTICIÓN

Se le llama a la condición parcialmente reversible en la que la partición es visible a través del *software* “*diskmgmt.msc*” y, en adición, presenta los siguientes síntomas:

1. El disco lógico muestra que contiene un SA tipo RAW [101].
2. Al igual que en el caso de pérdida de partición, solicita al usuario la aplicación de un proceso de formato para la utilización del espacio de almacenamiento.
3. Muestra un error de acceso por diferentes circunstancias, siendo las más comunes la falta de formato adecuado y/o un error de entrada y salida en el dispositivo.
4. El daño se presenta una vez que el SO indica que el equipo no fue apagado de forma correcta la última vez que fue accedido.

De la misma forma en la que el sector RAP responde, el volumen lógico no podrá ser reparado mediante la utilización del mismo SO instalado en el DDE físico, pues, aunque la partición primaria que contenga al SO no se encuentre afectada y sea una periférica la que sí lo está, este tiende a colocar a las particiones libres (particiones que no están asignadas e identificadas con un DBL específico de inicio y fin) como un espacio en donde es posible guardar información; esto provocaría un estado de sobre escritura y corrupción de los datos almacenados y a su vez, inútil un proceso de reparación.

La problemática principal de este fenómeno es que los bloques de bytes de la partición conocidos como: “DBL total” y “tamaño” se encuentran corruptos, esto sugiere que el mismo SO no identifica la extensión de la partición y/o su distribución en bytes, al no conocerse su ubicación no es posible aplicar un método directo de recuperación. La problemática anterior se puede resolver utilizando el conjunto adyacente de particiones que rodean a aquella dañada, al ubicar el final e inicio de cada una de estas es posible, por consecuencia, identificar los datos restantes.

Cuando existe solamente una partición total en el DDE físico y no hay otras en contra de las cuales se pueda obtener la extensión de la primera; para estos casos, se utiliza el DBL total identificado en los datos de placa del DDE y, mediante el sistema CCS, se ubican los sectores iniciales y finales máximos disponibles para el AU, excluyéndose el AS.

Para ejemplificar la condición previamente descrita, en la figura 30, se muestra un esquema en el que las particiones 1 y 3 encuentran comprendiendo a la partición 2 que se encuentra dañada, para su ubicación específica se utiliza la última dirección en sistema DBL de la primera partición y la primera dirección de la tercer partición igualmente especificada en sistema DBL, al igual que la cantidad total de sectores del DDE.

PARTICIÓN 1	PARTICIÓN 2	PARTICIÓN 3
15830210	DESCONOCIDA	25621798
SECTORES.		SECTORES.

625142448 SECTORES

Figura 30. Utilización de particiones adyacentes activas para la identificación de un volumen dañado.

Una vez conocidos los sectores de los respectivos discos lógicos es necesario igualmente conocer la cantidad de sectores totales del DDE para conocer la distribución y ubicación de las particiones (para este caso, el DBL total corresponde a 625142448 sectores), posteriormente se podrá calcular los sectores restantes a través de la ecuación siguiente:

$$\zeta = \Psi - \Delta \dots (5)$$

De la ecuación (5), sus elementos se definen como:

ζ = Sectores indefinidos. Ψ = Sectores totales de la última partición.

Δ = Sectores totales de la primera partición.

Sustituyendo valores en la ecuación (5) se tiene que:

$$\zeta = 25621798 - 15830210 [\text{SECTORES}]$$

$$\zeta = 9791578 \text{ SECTORES}$$

El DBL será utilizado para, una vez conocido el tamaño en sectores de la partición, ubicar este en la dirección física a la que corresponde mediante el sistema CCS.

Conocer la ubicación de la partición, así como sus sectores límites inferiores y superiores ayudará en el proceso de restablecer el acceso a la información. La descripción del proceso

de reparación será a partir de la utilización de *software* y la ejecución de una consola de recuperación en un ambiente externo al SO dominante en la partición primaria.

DESCRIPCIÓN DEL PROCESO DE REPARACIÓN

Se observan, en la tabla 20, los datos de placa (y lógicos) de un DDE con daño consistente en la tabla de particiones secundaria (partición de datos) posterior a la partición primaria principal y anterior a la tercera partición secundaria.

La visualización del estado de las particiones es obtenida a partir de la utilización del *software* “*diskmgmt.msc*” (figura 31).

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	SEAGATE.
MODELO.	ST3250824AS.
DBL.	488397168 SECTORES.
INTERFAZ.	SATA.
CAPACIDAD DE ALMACENAMIENTO.	250 GB.
VOLUMENES CONTENIDOS.	<ul style="list-style-type: none"> • DISCO LÓGICO “D” (PARTICIÓN PRIMARIA). • DISCO LÓGICO “E” (PARTICIÓN SECUNDARIA DAÑADA). • DISCO LÓGICO “G” (PARTICIÓN SECUNDARIA).

Tabla 20. Datos de placa para DDE con daño consistente en la tabla de particiones.



Figura 31. Visualización del volumen lógico a través del *software* “*diskmgmt.msc*” para un daño consistente en la tabla de particiones.

En la figura 32, se observan los datos de placa para el DDE previamente mencionado, nótese que se especifica en la etiqueta principal que el dispositivo cuenta con un certificado de reparación por la misma empresa desarrolladora, esto implica que, previamente, este dispositivo ha fallado físicamente, esto es de especial relevancia puesto que se establece que el DDE no está operando en su totalidad, o bien, se encuentra modificado (física y lógicamente) para funcionar y almacenar información aceptablemente.

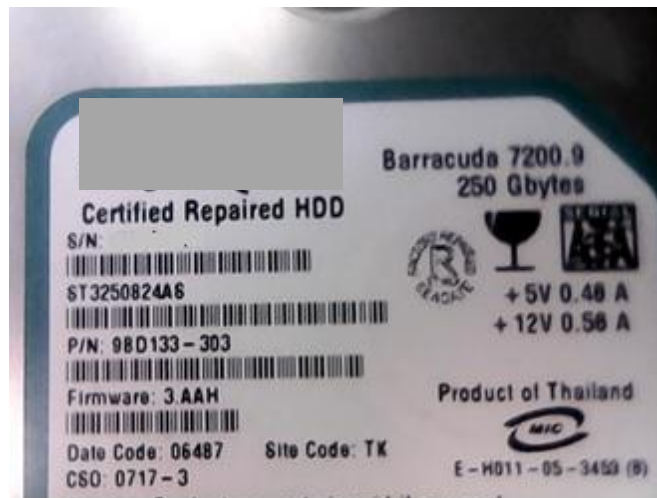


Figura 32. Datos de placa del DDE con daño consistente en la tabla de particiones.

Para el caso de estudio en particular de este DDE, el origen de su daño es del tipo lógico ocasionado por una condición física de naturaleza eléctrica. Existió un corte en el suministro de alimentación durante el proceso de modificación del volumen (expansión de una partición secundaria) y, al realizarse operaciones parciales por parte del programa “*diskmgmt.msc*” sobre la tabla de particiones, se produjo la corrupción descrita.

PROCEDIMIENTO

De forma genérica, la técnica de reparación empleada será a partir de la utilización de *software* semi-automatizado a través de una consola de recuperación externa en la que se garantice la integridad de las demás particiones adyacentes. A continuación, se procede a realizar la descripción de las ejecuciones del *software* mismo.

1. Ejecutar la consola de *software* con privilegios de administrador (de lo contrario no se podrán iniciar los módulos para obtener la propiedad del objeto analizado).

2. Crear un evento, es decir, un archivo en donde se almacenen temporalmente las modificaciones aplicadas a la estructura lógica.
3. En la consola debe de especificarse el tipo de volumen que se está conectado, para el caso de un daño consistente de partición esta siempre se presentará en formato tipo RAW; por lo tanto se procede a seleccionarse.
4. Mediante la ejecución de comandos, visualizar a manera de lista el conjunto elementos que se encuentran conectados físicamente al sistema computacional. Este punto del procedimiento es de crítica importancia ya que se mostrarán, primeramente, discos físicos y, posteriormente, los discos lógicos del volumen; alterar otro DDE podría o provocar una segunda corrupción en otra tabla adyacente.
5. Seleccionado el disco físico, especificar el tipo de partición que se desea recuperar. La selección implica definir la base del SA predominante, para el caso de equipo con estudiado, se identifica la tipo “PC, NTFS”. Para los casos en los que no sea posible definir el SA previo a la falla, se deberá ejecutar el comando de auto-detección que, basado en un algoritmo de programación, localizará la información y/o rastros de esta contenidos en el campo “tipo de partición”.
6. Definido el tipo de SA, ejecutar en la consola la instrucción de *software* para activar un análisis profundo en las particiones existentes, identificará entonces las primarias y secundarias, así como aquellas que se encuentren activas e inactivas.
7. La consola, configurada para hacerlo de forma automática, eliminará las entradas inválidas y acoplará nuevas (basándose en el DBL de las particiones adyacentes), de la misma forma, ubicará el sector de inicio de cada SA válido para confirmar anomalías en sus contenidos que condicionen la identificación del volumen ante el SO.
8. Una vez que las entradas han sido construidas, utilizando una consola secundaria, invocar el comando para mostrar en pantalla el conjunto de archivos (organizados en forma de directorios) acoplados al volumen. Identificados los volúmenes y corroborando que la información deseada se encuentra disponible, se guardan las modificaciones aplicadas.

Una vez aplicados los procedimientos anteriormente descritos, es necesario reiniciar el SO en el sistema computacional al que se encuentra conectado y, mediante el uso del *software* “*explorer.exe*”, [18, 47] visualizar la partición restaurada.

El evento de que la partición no sea visible posterior a la aplicación de la técnica, sugiere entonces que el problema, en un inicio lógico, se ha extendido hasta ser un daño físico, la solución directa sería restaurar por completo el sector RAP (de no ser posible, la pérdida de la información sería completa pues no existe ningún sector de inicio que descargue la secuencia de carga correspondiente).

Para el caso particular del DDE candidato a la reparación, el daño no se consideró en dicho sector y la tabla ha sido restituida en sus entradas. En las figuras 33 y 34 se observa, respectivamente, el disco lógico recuperado mediante la utilización del *software* “*diskmgmt.msc*”, así como la apertura de la carpeta principal mediante el “*explorer.exe*”.



Figura 33. Visualización del volumen lógico a través del *software* “*diskmgmt.msc*” para una restauración exitosa por daño consistente en la tabla de particiones.

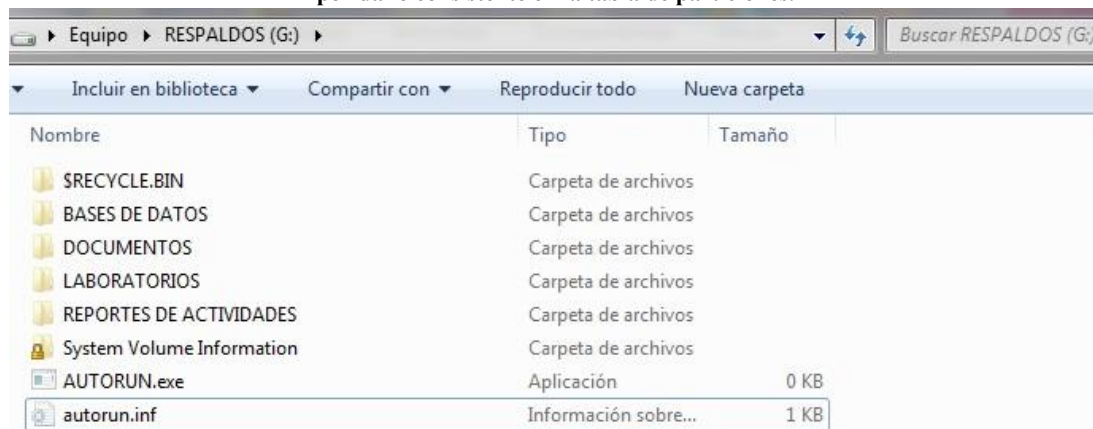


Figura 34. Visualización del volumen lógico a través del *software* “*explorer.exe*” para una restauración exitosa por daño consistente en la tabla de particiones; inaccesible por causa de *software* malicioso.

De la figura 33, se observa que todo el conjunto de particiones se identifican como “primarias”; se ha establecido que este tipo de particiones permiten el almacenamiento de un SO, pues, ya que contienen un sector RAP y una tabla de particiones, sin embargo, se

podrán contener múltiples tablas de particiones del tipo primarias siempre y cuando se cumplan las siguientes condiciones:

1. Cuando el *software* BIOS identifique cada uno los sectores RAP y sus respectivas tablas de particiones, deberá ejecutar solamente aquella activa que contenga al SO principal que, de acuerdo a la configuración de la interfaz de conexión, estará definida en la información de inicio del BIOS mismo.
2. Solamente se leerán aquellas particiones con el indicador “activo”, las otras serán consideradas como de almacenamiento de datos.

A continuación, en la tabla 21 se muestra, de forma condensada, el conjunto de operaciones y resultados obtenidos a partir de la implementación del método de reparación expuesto.

ELEMENTO	TIPO DE DAÑO/CARACTERÍSTICAS	MÉTODO APLICADO	RESULTADOS
CORRUPCIÓN DE LA TABLA DE PARTICIONES	LÓGICO, CON IMPOSIBILIDAD DEL USUARIO PARA INICIAR EL SO Y/O ACCEDER A LA INFORMACIÓN.	REPARACIÓN SEMI-AUTOMATIZADA POR COMANDOS A TRAVÉS DEL USO DE LA CONSOLA DE RECUPERACIÓN EXTERNA.	RECUPERACIÓN PARCIAL.

Tabla 21. Componentes de la tabla de particiones, errores, método de solución y resultados.

CONCLUSIONES PARCIALES

En esta sección se observó el comportamiento antes, durante y después de la aplicación de un método de reparación semi-automatizada por *software* aplicado a un DDE, el cual, contenía corrupciones en su tabla de particiones de su sector de inicio principal. Se utilizaron los *softwares* “*diskmgmt.msc*” y “*explorer.exe*” para visualizar y acceder a la información una vez restaurados todos los parámetros de operación necesarios.

Existen escenarios de restauración de datos en los que la tabla de particiones y/o la TMA son totalmente irrecuperables, esto debido a que (por diferentes razones de *hardware* y *software*) una significativa cantidad del código representativo de cada uno de sus módulos

se encuentra totalmente alterada a tal magnitud que no existe la suficiente información interna como para reconstruir las estructuras.

El escenario estudiado, pese a que se permitió el restablecimiento del objeto analizado, no puede ser catalogado como una recuperación completamente exitosa, pues, la información allí contenida aún se encuentra inaccesible a causa de la ejecución en estado permanente de *software* malicioso tipo “virus informático” (figura 34). En la sección siguiente se estudiarán el conjunto de estragos identificables en una arquitectura de SO provocados por este tipo de objetos, de igual forma, aquellos métodos de reparación típicamente utilizados. De forma complementaria, para establecer un escenario completo de recuperación, se continuará dicho proceso de recuperación de información en el objeto de estudio especificado en la figura 32 del presente capitulado (ver página 216).

2.1.3 CASO REPRESENTATIVO 3: CORRUPCIÓN DEL SISTEMA OPERATIVO A CAUSA DE INFECCIONES POR *SOFTWARE* DEL TIPO “VIRUS INFORMÁTICO”

La dinámica básica de funcionamiento interna del DDE contempla fundamentalmente los siguientes elementos:

1. Elementos lógicos, eléctricos y electrónicos.
2. Dispositivos mecánicos.
3. Módulos de *software* para ejecutar instrucciones de control (SO).

En las secciones anteriores se han analizado aquellas condiciones lógicas que afectan la capacidad del DDE para poder acceder a su contenido máspreciado: la información de usuario y el SO. Sin embargo, existen una serie de elementos externos al DDE que comprometen dicho funcionamiento al grado en el que, sin afectar su programación nativa y/o dispositivos mecánicos, la información puede ser degradada y hasta destruida; por lo tanto, cuando se implementa un procedimiento de recuperación de datos es esencial aplicar un proceso de extracción que, de igual forma, permita que los grupos de bytes obtenidos contengan índices de calidad aceptables para ejecutar su posterior edición.

El objetivo medular del presente proyecto de investigación consiste en la producción de todo el conjunto de condiciones físicas y lógicas que permitan la extracción íntegra de la información a partir de la implementación del *software* de diseño “FERCUVILL V5.0”, bajo un ambiente de ejecución de SO. Atendiendo al objetivo mencionado, resulta necesario primeramente definir aquellos elementos (y subelementos constitutivos) principales implicados en los procesos de lectura, escritura, asignación de directorios y, dentro de estos, sus respectivas problemáticas características al igual que sus respectivos métodos de recuperación.

SISTEMA OPERATIVO (SO)

Se define como aquella plataforma lógica y virtual de administración, operación y control por *software* para la manipulación del *hardware* en la que tienen evento todas aquellas interacciones de programación de subelementos secundarios (otros programas) en un ambiente controlado (típicamente) a través de una interfaz gráfica y/o consola de comandos principal [27, 32, 47].

ESTRUCTURAS CARACTERÍSTICAS

De forma genérica, un SO contiene una infraestructura tal que le permite realizar operaciones de interacción con dispositivos internos y externos a través de protocolos de “Entrada y Salida” (E/S) [38, 42] con señales de diferentes naturaleza (analógicas y digitales), es decir, todos aquellos circuitos físicos (*hardware*) propios y ajenos al sistema nativo conectados a través de puertos; comunicados y controlados por medio de buses.

A continuación, en la tabla 22, se presenta la división estandarizada para *softwares* del tipo SO; el criterio utilizado es a partir de una arquitectura multiprocesos [70].

ELEMENTO	DESCRIPCIÓN
NÚCLEO.	Componente encargado de la transformación y disposición directa de los recursos reales en recursos virtuales para un sistema computacional. La relación de

	<p>control hacia <i>hardware</i> es llevada a cabo por medio de la generación de procesos ejecutables que, adicionalmente, se les asigna un espacio en memoria, tiempos de ejecución y término y, de ser necesario, memoria complementaria. De la misma forma, el núcleo concede la creación de “árboles de subprocesos” que administran de forma particular los recursos asignados para cada proceso ejecutable del sistema.</p>
<p>INTERFAZ DE PROGRAMACIÓN DE APLICACIONES (IPA).</p>	<p>También conocido como “bloque de instrucciones por lote”. Se define como aquel conjunto ordenado de paquetes lógicos que ejecutan rutinas y subrutinas (basadas en un lenguaje de programación) de forma periódica cuando un objeto de mayor jerarquía les invoca.</p> <p>La definición de la IPA, aplicado a la arquitectura de SO, puede referirse como aquel conjunto de protocolos suficientes que permite comunicar a una o varias aplicaciones de <i>software</i> residentes en el SO.</p> <p>El contenido de la IPA debe de ser compatible con cada uno de lo <i>softwares</i> (y sus respectivos procesos) a fin de que se ejecute y opere de forma estable cuando sea cargado en memoria.</p>
<p>CONTROLADOR.</p>	<p>Conjunto de instrucciones lógicas programables que, mediante un diseño de control de variables, permiten la ejecución</p>

	<p>de: identificación, control, monitoreo, apertura y cierre, actualización y edición de todo el conjunto de <i>software</i> necesario para establecer una comunicación que gobierne distintos elementos físicos internos y externos al sistema computacional. Este es el componente medular al momento de conectar (por medio de una interfaz de control) unidades de DDE, memorias de interfaz USB y/o cualquier otro circuito periférico [63].</p>
<p>SISTEMA DE ARCHIVOS (SA).</p>	<p>El SA es el componente local del núcleo que ha de multiplexar un DDE de tamaño identificado en un orden de dispositivos lógicos identificables por medio de una interfaz (gráfica y/o por línea de comandos). Dentro de dicha organización, las estructuras encontradas son: volúmenes, directorios, carpetas, archivos y aplicaciones ejecutables.</p> <p>El núcleo utiliza las siguientes instrucciones residentes para invocar el SA de forma autónoma, local y remota:</p> <ul style="list-style-type: none"> • <i>Open</i>: permite conceder el acceso al objeto seleccionado. • <i>Read</i>: habilita la capacidad para, mediante la utilización de un intérprete de datos, leer y acceder al contenido de un objeto en particular. • <i>Write</i>: concede los permisos para que un objeto, previamente leído su

	<p>contenido, pueda ser manipulado en alguna de sus líneas de contenido.</p> <ul style="list-style-type: none"> • <i>Close</i>: concede la finalización de una rutina, un objeto (carpeta o archivo) y/o cualquier otro elemento lógico administrado y ejecutado por el SO. Este proceso se realiza de forma tal que, independientemente del momento en el que se ejecute la instrucción, el contenido no sea corrompido a causa de un cierre inesperado. • <i>Lseek</i>: comando con altos privilegios de control encargado del posicionamiento del cabezal por sobre encima de un bloque de datos predeterminado. Esta instrucción ofrece la posibilidad de que un objeto específico, aunque se encuentre distribuido en diferentes localidades físicas, sea identificado y “unido” lógicamente para aplicarle posteriores procesos tales como: acceso, edición y finalización.
<p>INTÉRPRETE DE COMANDOS.</p>	<p>Es el proceso multitarea no nativo del núcleo que se encarga de la lectura y ejecución de todas las instrucciones interactivas que acontecen en el SO (ya sea que estas sean invocadas por el usuario y/o solicitadas por un <i>software</i> externo).</p>

Tabla 22. Arreglo estandarizado para los elementos estructurales del SO.

Los *softwares*, aplicaciones y/o programas del tipo “virus” tienden a alterar de forma parcial y/o total los elementos descritos en la tabla 22 (siendo los más recurrentes el SA y la IPA); la velocidad, especificidad y extensión de los daños perpetrados a la información dependen directamente, tanto de la complejidad del diseño mismo como del tipo en concreto del que se esté propagando.

Para implementar las debidas medidas de recuperación, protección y prevención, es necesario conocer primeramente la definición y conjunto de operaciones que estos tipos de programas poseen. Así pues, en la tabla 23, se procede a exponer y, esencialmente, mencionar aquellos campos de interés más representativos, directos e identificables para el presente proyecto de investigación.

VIRUS INFORMÁTICO

Este se define como aquel *software* compilado cuyo código de programación atenta de forma directa y/o indirecta la información a partir de la alteración, adición, interferencia, exclusión y/o borrado de todo aquel proceso nativo perteneciente a la dinámica lógica de funcionamiento de un SO y física de un DDE, tanto con sus elementos internos como externos.

Estos tipos de programas se encuentran orientados, funcionalmente, a la perturbación de líneas de código estratégicas localizadas en ciertas zonas del SO. Dichas líneas de código pueden referirse a las directivas de acceso, propiedades y contenido del archivo (información), siendo este último el más importante dentro de un marco de recuperación de datos, pues, puede ser de carácter parcial y/o permanente.

Los virus informáticos, al no ser programas que originalmente pertenecen al SO, tienden a adherirse a algún objeto específico (típicamente archivos y/o programas ejecutables), dicho proceso es conocido como **infección** y, por cuestiones de diseño, los archivos infectados se ven forzados a operar en estado permanente (sean o no sean invocados por el SO y/o el usuario) para evitar ser eliminados; esto es, ya que cuando un objeto que se encuentra en uso no es posible editarlo, cambiar su ubicación, renombrarlo y/o eliminarlo.

Otro tipo de comportamiento visible en este tipo de aplicaciones es la falta/ausencia de propiedades referentes al tamaño del archivo, algunos *softwares* antivirus [93] tienden a omitir de su análisis a aquellos objetos cuyo peso sea igual a 0b (ya que se asume que al no contener un peso tampoco puede existir código), con ello, los procesos de detección y desinfección se tornan aún más complejos.

En la figura 35 se observa un mensaje de error del SO cuando se intenta eliminar un archivo ejecutable (para este caso en particular, el objeto citado es creado y replicado de forma automática por un código malicioso almacenado en el archivo “autorun.inf” y no pertenece a las carpetas y contenidos de las mismas), nótese que el objeto que se intenta eliminar pertenece precisamente al planteado en el caso de estudio número 2, específicamente el de la figura 42.

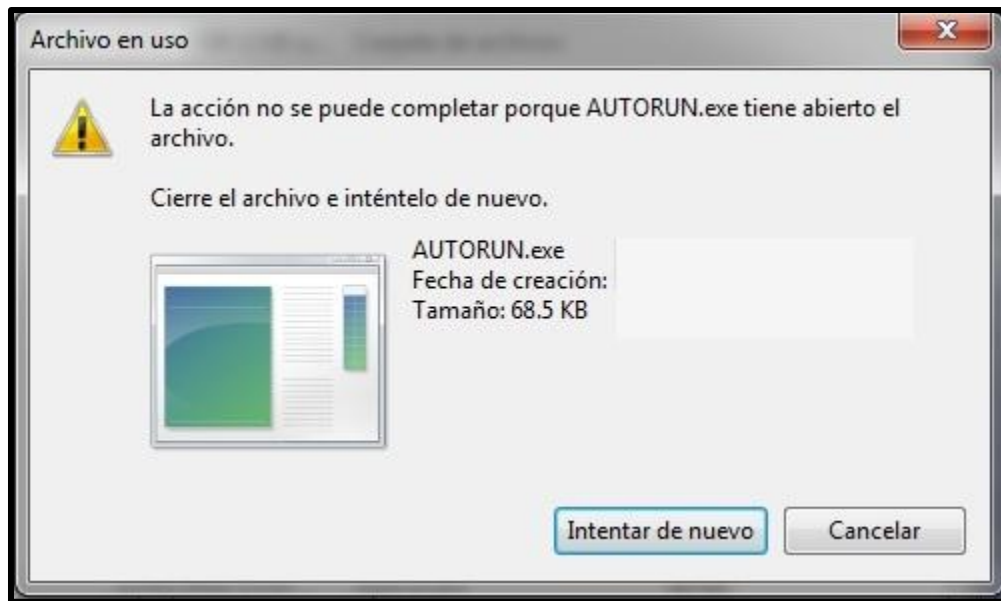


Figura 35. Visualización del mensaje de advertencia del SO ante la incapacidad de eliminar un archivo malicioso.

De las figuras 34 y 35, respectivamente, puede observarse que, para la primera de estas, el del tamaño del objeto se encuentra expresado por 0 KB (“Kilo Bytes”), en tanto que para la segunda se observa un peso de 68.5 KB; dichas discrepancias sugieren que, además de la alteración de la propiedad “tamaño”, el *software* “*explorer.exe*” también se encuentra afectado; esto implica que, tanto objetos infectados como no infectados estarán sujetos a falsas lecturas para dicha propiedad. (Ver el “CASO DE ESTUDIO 1” con “FERCUVILL V5.0”).

CLASIFICACIÓN DE LOS VIRUS INFORMÁTICOS

El estudio para esta sección se llevará a cabo definiendo cada elemento particular y mencionando su respectivo comportamiento. **Los virus informáticos, para los fines del presente proyecto, pueden ser clasificados de forma general de acuerdo a lo expresado en la tabla 23:**

VIRUS INFORMÁTICOS		
CARACTERÍSTICAS DE OPERACIÓN	MÉTODOS DE PROPAGACIÓN	CÓDIGO DE PROGRAMACIÓN
<p>1. CONSUMO DE RECURSOS.</p> <p>2. CONSUMO DE ESPACIO ASIGNADO.</p>	<p>3. INSTALACIÓN FRAUDULENTO.</p> <p>4. ADQUISICIÓN POR NODOS DE RED.</p> <p>5. COMPORTAMIENTOS.</p>	<p>6. CABALLO DE TROYA.</p> <p>7. GUSANO.</p> <p>8. MACRO BLT.</p> <p>9. VIRUS “ERS”.</p> <p>10. VIRUS DE PROGRAMA.</p> <p>11. VIRUS DE INICIO.</p> <p>12. VIRUS DE DIRECTORIO.</p> <p>13. VIRUS POLIFÓRMICO.</p> <p>14. VIRUS “HOAX”.</p>

Tabla 23. Clasificación general de los tipos de virus informáticos actuantes en el SO.

❖ CARACTERÍSTICAS DE OPERACIÓN

Esta propiedad se define como todo aquel conjunto de dinámicas, técnicas, puntos de vulnerabilidad, algoritmos de programación y capacidades de propagación que los *softwares* del tipo “virus informático” utilizan para obtener propiedad por sobre un SO, sistema computacional y/o DDE de forma permanente hasta que cumplan las siguientes condiciones:

1. Aniquilación y/o descomposición de las estructuras lógicas encargadas de mantener la información resguardada en un *software* de mayor jerarquía.
2. Apropiación de los recursos y capacidades físicas del equipo infectado para fines secundarios a los que el usuario no tiene conocimiento.
3. Hasta que se logren ejecutar todo el conjunto de actividades para las cuales el programa fue originalmente diseñado.

Para los fines del presente proyecto, existe una dupla de características de operación que resultan de especial interés; la razón, es que debido a estas existe la mayor corrupción de datos y/o vulneraciones hacia la información. A continuación, se muestra dicho conjunto y sus consecuencias/características directas.

CONSUMO DE RECURSOS

Este término engloba de forma general todos aquellos medios eléctricos, electrónicos y mecánicos de lo que se vale un equipo computacional para ejecutar sus funciones. Para cada uno de los tipos de programas maliciosos y de sus las diferentes variantes, es que tendrán comportamientos únicos, siendo los siguientes los más relevantes para el estudio desarrollado:

Software

- Saturación de la memoria virtual, RAM (tanto del sistema computacional como la interna del DDE).
- Corrupción de la información del *software* BIOS a partir de la alteración física de las memorias, según el caso, tipo ROM y/o **EEPROM**.
- Usurpación y utilización del ancho de banda de red para fines distintos a los que el SO y/o el usuario dispondrían, por ejemplo: la creación de un punto de acceso fraudulento para filtrar información bancaria y/o violación de la privacidad al obtener de forma ilegítima claves y nombres de acceso hacia ciertos sitios cibernéticos.
- Saturación de la capacidad máxima de almacenamiento de datos en un DDE y, de ser posible, un proceso de sobre-escritura forzada en zonas de altos privilegios pertenecientes al AS y AU.

- Corrupción del conjunto de *software* del tipo “controlador” para propagar de forma inadvertida el código malicioso.

Hardware

- Destrucción física de elementos mecánicos por causa de instrucciones cíclicas en sus circuitos de control referentes.
- Fallos en los protocolos y módulos de control eléctricos y de temperatura para que, de forma progresiva, el desgaste en el material sea acelerado y/o exista una carbonización directa de elementos como: microprocesador, memorias digitales y/o tarjetas de video nativas y externas.
- Variación deliberada en las frecuencias de operación (presencia de armónicos) para deteriorar el material conductor eléctrico.

Pese a que el diseño de estas aplicaciones está orientado a actuar directamente sobre el *software* local de un equipo de cómputo, esto no significa que el *hardware* no pueda verse afectado de forma indirecta. Esencialmente, el código malicioso implementará cualquier medida que permita ejecutar cortes sustanciales en cualquier medio y/o sistema de transmisión y recepción de información.

CONSUMO DE ESPACIO ASIGNADO

El DDE, como ya se ha mencionado anteriormente, contiene una estructura lógica básica en la que define direcciones en las cuales es permitido y no guardar información. Básicamente, la directriz principal es que ningún objeto puede ocupar, en un mismo tiempo, un mismo espacio físico y lógico. Sin embargo y en la presencia de virus informáticos, dicha directriz tiende a ser la primera vulnerada y, con ella, los datos contenidos en el DDE.

El proceso de sobre-escritura de datos consiste en el empalme del contenido en sectores de valores y/o datos binarios consecutivos en espacios físicos y lógicos cuyo contenido no se encuentra marcado como “disponible”; cuando este sucede, formalmente se expresa una corrupción en la información. **Desafortunadamente para el usuario, dichos cambios no son reversibles y, de ser detectado a tiempo, sólo podrán realizarse procedimientos parciales de recuperación de datos contenidos en el disco lógico.**

❖ MÉTODOS DE PROPAGACIÓN

En este apartado se estudiarán las principales formas de proliferación de los virus informáticos, tanto físicas como lógicas, y así mismo, se analizarán el conjunto de técnicas y criterios utilizados para invadir y posesionarse de objetos exclusivos y nativos de un SO.

Los **métodos de propagación** se definen como todas aquellas formas, medios físicos y virtuales a través de los cuales el código malicioso puede insertarse en un objeto secundario externo durante un momento y evento determinados. Debe de entenderse la palabra “momento” como las constantes de tiempo en el que ocurre la infección y “evento” como la actividad (apertura, ejecución o cierre) presente en el que el objeto al instante de la alteración en sus líneas internas de algoritmo.

Un SO comenzará a experimentar cambios en su dinámica de funcionamiento cuando se encuentre invadido por algún otro *software* que no se encuentre registrado dentro de sus parámetros nominales de operación.

A continuación, se proceden a explicar dichos métodos, así como sus características propias.

INSTALACIÓN FRAUDULENTA

Este consistía en hacer partícipe al usuario en el proceso de infección mediante la sugerencia sobre la instalación de un *software* de protección de antivirus, el cual, una vez residente del equipo, informaba sobre la existencia de múltiples amenazas identificadas; (dichas “amenazas” correspondían a archivos del SO y/o mostraban rutas y carpetas inexistentes). Posteriormente, el usuario procedía a iniciar el supuesto análisis y como resultado de este se obtenían nuevas zonas del DDE infectadas.

Los objetivos de estas variantes modificados de *software* son múltiples, sin embargo se destacan los siguientes:

1. Obtener ingresos económicos simulando la adquisición de la versión completa del producto, la cual, podía “eficientemente” eliminar los archivos infectados.

2. Bloquear rutas de acceso de información vitales para el usuario, obligándolo entonces a adquirir un servicio de desinfección, en ocasiones, proporcionado por la misma empresa desarrolladora del “antivirus”.

El ejemplo ideal para este tipo de elementos es el llamado “Antivirus 2010” [67, 68] (figura 36), el cual aseguraba brindar un supuesto y completo esquema de protección integrando múltiples tecnologías de heurística avanzada y protección en tiempo real.

Los estragos identificables por el *software* “Antivirus 2010” son:

- Descomponer el contenido de archivos con extensiones: “.doc, .docx”, es decir, documentos de texto.
- Presentar mensajes en pantalla invasivos, los cuales, evitaban la navegación y uso de las herramientas nativas del SO y *software* legítimos instalados.
- Obtención de información confidencial del usuario a través de métodos ilegales.



Figura 36. Interfaz de control principal para el *software* “Antivirus 2010”. Tomado de: [67]

En la actualidad, la presencia de este tipo de amenazas ya es identificada de forma eficiente como falaz y, por dicha razón, estos son cada vez menos frecuentes. Sin embargo, el programa “Antivirus 2010” y sus similares establecen un precedente sobre el tipo de recursos y medios aparentemente inusuales que pueden ser explotados para vulnerar los diferentes sistemas de seguridad.

ADQUISICIÓN POR NODOS DE RED

Este se define como aquella capacidad del código malicioso para, además de infectar el SO del DDE de forma local, lograr transmitirse a través de los puntos de acceso hacia las diferentes conexiones en red locales y foráneas.

Los principales puntos de infección de los sistemas en red son:

- Sistemas de mensajería de correo electrónico y sistemas de bases de datos con arreglos de intranet.
- Acceso a servidores cuya certificado de autenticidad sea deficiente, inexistente y/o de procedencia desconfiable.
- Utilización de puertos de acceso exclusivos para mantenimiento del *hardware* relacionado con el servicio de red instalado. Dichos puertos, al suponerse como normalmente inaccesibles, no cuentan con protocolos de protección y son vulnerables ante ataque cibernéticos.

La incidencia y número de amenazas relacionadas a los nodos ha aumentado considerablemente (usuarios domésticos) desde que existen servicios de red masivos; sin embargo, anteriormente la principal vía de propagación de estos programas era a partir de dispositivos digitales como “*diskettes*”, discos multimedia en formato CD y DVD, así como unidades de almacenamiento masivo de formato USB y discos externos; lo cuales, al ser abiertos sus contenidos, rápidamente identificaban el punto de acceso hasta la siguiente dirección de red disponible para ser infectada. Los propósitos para las distintas versiones de programas que utilizan esta forma de propagación son variados, se destacan aquellos que bloquean el acceso a archivos del SO y/o los que, en adición, eliminan su contenido y lo suplantán con datos de patrones aleatorios.

COMPORTAMIENTOS

En este apartado se estudiarán las tendencias que múltiples algoritmos de programación pueden adoptar para asirse a objetos secundarios, para con ello, lograrse infiltrar al SO de forma tal que se mantenga la integridad del código primario mismo [92].

Empalme:

Técnica exclusiva de los virus para empatar su código de programación entre las líneas de código del objeto al que secuestra. La adición del código malicioso no daña el código original del objeto afectado ya que, mediante una instrucción en su diseño, este se añade en el último bloque posible inmediato.

Inserción:

A diferencia del anterior, este procedimiento consiste en la escritura forzada del código vírico en zonas reservadas, no sólo del objeto que infecta, sino del SO y del DDE mismo, tales como en AS y/o sectores que han sido excluidos por el módulo *firmware*. Dicho proceso daña significativamente la programación inicial de la zona invadida y sus adyacentes.

Redireccionamiento:

Su principio es el de la “inserción”, consiste en que el código base (principal) se almacena de forma permanente en un sector físico, en tanto que otras subrutinas del mismo programa invaden otros objetos. El proceso infeccioso comienza formalmente cuando estas subrutinas invocan al *software* principal para comenzar a eliminar, de forma permanente, el contenido de sectores contiguos adyacentes.

Compactación:

Es aquella tecnología de protección ante la detección que algunas variantes de virus informáticos utilizan para evitar ser borrados. Consiste en la generación de un código cifrado (complejo algoritmo de identificación) dinámico, con ello, los *softwares* de antivirus son incapaces de observar patrones repetitivos y lo asumen como (aunque desconocido) otro archivo del sistema.

Sustitución:

Es el comportamiento reportado como más agresivo y destructivo en términos informáticos. Consiste en el borrado del código original del objeto infectado, solamente se mantienen ciertas líneas que permiten al SO reconocer dicho objeto como válido para seguirlo utilizando; el nuevo contenido resulta ser el código malicioso y, cuando es invocado para ser ejecutado, este será capaz de infectar nuevos elementos de distintas locaciones. A cambio, el SO recibirá en respuesta un error de comunicación entre este y el objeto ejecutado.

❖ CÓDIGO DE PROGRAMACIÓN

Se define como aquel arreglo de instrucciones lógicas capaz de promover ejecuciones, aperturas, cierres, modificaciones y/o cualquier otra directiva administrativa que directamente pueda controlar un módulo de lectura-escritura dentro de un SO.

Un *software* tipo “virus” adquiere dichos privilegios para que, sin impedimento alguno, pueda realizar las tareas para las cuales ha sido compilado. A continuación, se procede a explicar aquellos tipos más representativos conjunto a sus características de operación.

CABALLO DE TROYA

También conocido como “troyano” [76], este *software* se instala como un complemento que, de acuerdo a su apariencia gráfica, se refiere a cualquier otra aplicación segura y/o con certificados de autenticidad, sin embargo (y una vez que se encuentra de forma residente) este programa adquiere control total causando los siguientes estragos:

CARACTERÍSTICAS DE COMPORTAMIENTO

- Administración local y remota de periféricos internos (DDE, memoria RAM, memoria ROM) y externos (memorias digitales y dispositivos multimedia conectados a través de los puertos del sistema computacional tales como USB, CD, DVD, cámaras de video, entre otros), así como de puntos de acceso no permitidos por la instalación de la red en el equipo afectado.

- Modificación de los atributos de identidad para ser presentado como un archivo propio al SO nativo.
- Utiliza a los puertos USB como principal vía de propagación a nivel local.
- Permite capturar las pulsaciones de teclado, visualización en pantalla e incluso el secuestro de identidad (del usuario) a partir de la obtención de datos como: nombres completos, direcciones de correo electrónico, domicilios, contraseñas cifradas e identificadores personales como lo son los archivos de extensiones “.cer y .key”, al igual que certificados de sellos digitales.
- Secuestro de identidad del equipo anfitrión, esto es, usurpan los recursos de *software* y *hardware* del equipo afectado y, mediante un arreglo de servidores, administran actividades ilícitas en las cuales el equipo secuestrado sea el identificado y no el que originalmente practica dicha actividad ilegal.

Por su conjunto de comportamientos, este tipo de programa es considerado uno de los más perjudiciales, ya que atenta directamente en contra de las políticas de privacidad de los usuarios de sistemas computacionales [86].

GUSANO

También llamado como “virus WRM”, se define como una infección cuya finalidad principal consiste en la sobrecarga del *hardware* perteneciente al equipo anfitrión (memoria virtual y memoria RAM, *software* BIOS y circuitos del DDE) mediante la reproducción del mismo en diferentes localidades, imposibilitando así el uso del sistema computacional. Este tipo de amenazas están diseñadas básicamente para que, una vez el equipo se encuentra en un punto de colapso, se le informe al usuario sobre la posible solución de dichos problemas mediante la instalación de algún *software* adicional (fraudulento) el cual sólo tiene como objetivo explotar económicamente al comprador sin ofrecer, evidentemente, una solución real.

CARACTERÍSTICAS DE COMPORTAMIENTO

- Capacidad autónoma de auto-replicación sin la necesidad explícita del usuario para ejecutarlos.

- Capacidad para secuestrar un servidor de mensajerías de correo electrónico y replicar su código hacia otras direcciones ajenas al equipo afectado.
- Secuestro consistente del ancho de banda del equipo local, típicamente utilizado para enviar información de reportes y estados de la infección hacia los desarrolladores del código malicioso.
- Deterioro, generación de estrés eléctrico y merma gradual en las capacidades físicas del equipo contenedor.

Este tipo de programa no afecta la información, estructuras o cualquier otro módulo de datos del usuario y/o del SO; por ello, el sistema computacional opera con relativa estabilidad por largos periodos de tiempo cuando se encuentra influenciado por este [86].

MACRO BLT

También identificados como “bombas lógicas y/o TMR”, se define como una amenaza capaz de modificar el contenido programable de una subrutina de datos que los *softwares* principales utilizan para realizar procedimientos básicos. Esencialmente un programa TMR modificará una capacidad alguna de la cual se vale en específico otra aplicación para operar de forma regular, por ejemplo: la capacidad de abrir un documento, de realizar operaciones matemáticas básicas, editar el formato y tipos de arreglos de un procesador de textos e incluso modificar el comportamiento de dispositivos periféricos como el teclados y cursores.

Este tipo de programas no deben de ser confundidos con los **complementos macros**, los cuales, son herramientas adicionales que se añaden a un *software* de mayor jerarquía para permitir complementar y ejecutar nuevas funciones y tareas para las cuales (los *softwares* bases) no fueron originalmente desarrollados.

CARACTERÍSTICAS DE COMPORTAMIENTO

- Modificación del mapa de teclado y comandos asociados; esto es, los métodos de abreviaturas quedan deshabilitados y son intercambiados por otros que deterioran el contenido del documento (típicamente los programas más afectados son los ya

mencionados procesadores de textos, pero también las hojas de cálculo y editores de bases de datos).

- Capacidad de deterioro de archivos que no se encuentran en ejecución, es decir, el virus podrá desintegrar los contenidos de objetos que no estén actualmente siendo editados; ya que estas amenazas identifican a sus elementos por medio de extensiones, por lo tanto, para procesadores de texto (“.doc” y “.docx”), hojas de cálculo (“.xls” y “.xlsx”), bases de datos (“.mdb”) y presentaciones gráficas (“.ppt”, y “.pptx”) sus contenidos se encuentran en grave riesgo de ser eliminados y/o corrompidos.
- Al igual que los virus “WRM”, estos son capaces de secuestrar un servidor de correo electrónico para efectuar su proceso de infección hacia otros sistemas computacionales de diferentes redes.
- Su diseño permite que los recursos que explotan no dependan del SO instalado, sino del *software* de mayor jerarquía que secuestre y, de esa forma, se le identifique como un complemento y/o herramienta; por ello es que los programas antivirus tendrán ciertas limitaciones al detectarlos, pues, no es regular que se identifiquen amenazas en productos registrados.
- Conjunto a los tipo “troyanos”, su principal vía de propagación es a través de los dispositivos interconectados a los puertos USB (memorias digitales y arreglos de DDE externos).
- Tienden a deshabilitar los mensajes de advertencia, solicitud y negación referentes a la instalación del complemento, de esa forma el usuario nunca podrá tener conocimiento de que ya se encuentra afectado.

Esta amenaza es la que, para dentro de un marco de recuperación, restauración y reparación de datos, representa uno de los principales riesgos (conjunto a los virus “troyano” y “ERS”, el cual se expondrá a continuación) ya que no sólo deteriora la información mediante un prolífico medio de propagación externa como lo es un servidor de mensajería electrónica, sino que imposibilita el uso de una de las principales vías de transferencia de información a nivel local: los dispositivos de interfaz USB [19].

VIRUS “ERS”

Conocidos igualmente como “eliminadores”, dicho *software* obedece a su nombre y se encarga esencialmente de la destrucción de arreglos de cadenas de datos internos a cada uno de los identificadores de los archivos, es decir, destruye solamente los contenidos y mantiene la extensión del mismo intacta. Un síntoma inequívoco de que el objeto infectado ha sido afectado total o parcialmente es que en su contenido solamente se muestran vestigios y/o restos parciales de la información original, o bien, se muestra como dañado.

CARACTERÍSTICAS DE COMPORTAMIENTO

- Los elementos afectados no se ven modificados en tu tamaño, esto es, ya a medida que el contenido es desaparecido, el virus “ERS” lo sustituye con su propio código.
- El código se incrusta en el elemento conocido como “cabecera”, el cual es un área reservada de cada archivo con el cual el SO es capaz de identificar ciertas características como: tipo de extensión, propiedades de lectura y escritura, localización física y lógica. Al encontrarse en este sensible zona, su desinfección es imposible y la única opción viable es la destrucción del archivo que lo contiene; **este punto conforma un estado en el que la recuperación es totalmente nula.**
- Se desplaza de forma tal que, para garantizar cierta recuperación parcial, se debe de extraer de forma manual (si y sólo si el archivo aún es editable) la información contenida y colocarla en una localidad externa, la cual, nunca haya tenido contacto con el sistema computacional residente.

A continuación, en la figura 37, se observa el cuadro de diálogo propio para un archivo de extensión “.docx” dañado e irrecuperable en su contenido a causa de esta clase de infecciones.

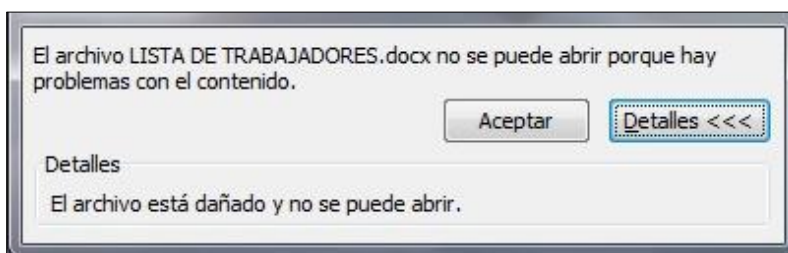


Figura 37. Visualización del mensaje de estado de error al abrir un archivo de extensión “.docx” deteriorado por la acción de *software* tipo “ERS”.

Estos programas, al no contar con la capacidad de expansión a través de nodos de red, se propagaron inicialmente por medio de dispositivos de digitales como unidades de CD y DVD; sin embargo, se ha observado una incidencia creciente de procesos infecciosos a través de dispositivos de almacenamiento conectados por medio de puertos USB [69].

VIRUS DE PROGRAMA

Este tipo de aplicación se “adhiera” hacia cualquier otro archivo que contenga, primordialmente, las siguientes extensiones: “.exe”, “.com”, “.ovl”, “.drv”, “.bin”, “.dll”, “.ini”, “.inf” y “.sys”. Este *software* malicioso tiene como objetivo principal el deterioro del contenido del SO afectando periféricamente la información del usuario al destruir las estructuras básicas del sistema que lo contiene, las cuales, son las encargadas de la ejecución de operaciones de lectura y escritura de datos.

CARACTERÍSTICAS DE COMPORTAMIENTO

- Mantienen intacto el *software* principal al que se adhieren; típicamente se alojan en los bloques anteriores o posteriores al programa base (a partir de este es que comienza a degradar a los adyacentes).
- Son capaces de ceder el control durante la ejecución de los procesos de instalación y trabajo del *software* infectado, sin embargo, justo antes de que este finalice, una instrucción de réplica se activa de forma inadvertida e infecta otros archivos ubicados en el mismo directorio.

Los virus de programa, pese a que no atentan directamente a la información, son los responsables de crear estados de inestabilidad en los que el SO dañe y/o bloquee zonas de almacenamiento de datos normalmente accesibles por el usuario. La permanencia de los efectos producidos depende concretamente de un par de condiciones:

1. La existencia de la amenaza en alguno de los directorios del SO.
2. La capacidad interna (autoreparación) y externa (herramientas de restauración) del sistema para restablecer las condiciones óptimas de operación. Típicamente, con la eliminación del archivo infectado y la reinstalación de una versión no corrupta, el SO (y sus subelementos) podrán ser nuevamente funcionales.

VIRUS DE INICIO

Llamado también como virus de “arranque”, este código malicioso compilado ya ha sido mencionado (ejecutable “ZAccess”, una de sus múltiples variantes) previamente en la sección estudiada: “SECTOR RAP (FIRMA “0XAA55”, página 76) del presente trabajo de investigación. Este tipo de *software*, potencialmente, puede ser el más dañino de los que se estudien en este listado [12], esto es, ya que puede bloquear, eliminar e incluso destruir todo método lógico de acceso al sector RAP de inicio; si bien para el caso expuesto (en la tabla 18) la recuperación fue exitosa mediante un proceso de desinfección, esto no siempre sucede ya que este programa tiende a evitar que el *software* BIOS desencadene el conjunto de instrucciones que permitan la identificación del DDE y, a consecuencia directa, de su información almacenada.

Una característica única de este tipo de aplicación es, precisamente, que no es residente del SO sino del DDE, solamente lo utiliza para infectar una dirección física y, de ser posible, al *software* BIOS [41].

CARACTERÍSTICAS DE COMPORTAMIENTO

- Deteriora la estructura lógica del sector RAP y/o de los sectores contiguos, lo cuales se utilizan en ocasiones para guardar una copia de seguridad del sector RAP mismo para ser utilizada de forma posterior ante una condición de fallo.
- Puede modificar los valores de salida del DDE que son detectables por el *software* BIOS tales como: identificador y capacidad de las unidades conectadas a través de los puertos de control, orden de inicio de los elementos (puede omitir al DDE que contiene la información deseada a recuperar).
- Dependiendo de la variante a la que se someta el sistema computacional, podrá conceder acceso parcial al sector RAP pero destruirá la TMA y cada una de las tablas de particiones contenidas en el.
- Debido a que este *software* se encuentra almacenado en memoria de forma permanente, todos los dispositivos de almacenamiento de datos conectados durante de la energización eléctrica serán infectados de forma automática.

- Dependiendo de la variante instalada en el DDE, si es que esta permite el inicio del SO, las protecciones antivirus la detectarán como un tipo “WRM” y eliminarán las copias, sin embargo, al siguiente reinicio estas ya estarán nuevamente instaladas continuando un ciclo permanente de detección y eliminación cuyo objetivo es la destrucción física del medio de almacenamiento a causa del estrés mecánico producido en los componentes involucrados.

Los índices de contagio aumentaron de forma considerable desde el momento que los fabricantes de los circuitos y *softwares* que conforman el BIOS comenzaron evitar el uso de memorias digitales del tipo ROM a cambio de las **EEPROM** [75], por sus siglas en inglés que significan: “**Electrically Erasable Programmable Read Only Memory**”, es decir, “Memoria de Sólo Lectura Borrable y Programable Eléctricamente”. Dichos circuitos, al tener ahora la capacidad de ser programados en más de una ocasión mediante la utilización de un arreglo de transistor del tipo “MOS” y, en adición, siendo una memoria no volátil, rápidamente sucumbieron ante este tipo de amenazas.

A continuación, en la figura 38, se ejemplifica una infección en el código de programación del BIOS, nótese que los valores hexadecimales muestran un valor en texto corrupto.

CÓDIGO HEXADECIMAL							VALORES EN TEXTO						
5	0E	00	B7	HH	ZH	0E	☺	11	700000	77	77	77	
2	E4	88	00	91	E2	FE	Èã	`Qô	2õê	æ0	■		
3	C6	00	20	E2	FE	B4	©UU*	YÁ	Èã	0	■		
F	D6	33	DB	B7	80	53	óê	fãF	☺	í3	■		
8	53	51	51	51	68	01	âý,	h	▶	Là	■		
C	AC	00	00	00	CD	20	☼	©AQQ	ï	7	■		
4	05	FE	46	4D	EB	EE	◆	▶	fâ	~	■		
8	08	88	01	C6	00	80	©^	▶	ãFM	ç	ù		
7	87	D5	EC	0C	44	97	ê	■	ê	☺	☺		
A	66	27	53	00	01	00	ç	¹	ù	ç	¹		
0	40	00	43	49	48	20	h	©	A	©	2		
0	00	00	00	00	00	00	v1.2	TTIT					
0	00	00	00	00	00	00							

Figura 38. Visualización del estado de corrupción del *software* BIOS infectado por causa de *software* malicioso del tipo “inicio”. Tomado de [66].

VIRUS DE DIRECTORIO

Se define como aquel *software* capaz de modificar las direcciones físicas y lógicas de un fichero (objeto en específico que pertenece exclusivamente al SO y que el usuario sólo es capaz de utilizar indirectamente, más no de editar), de esa forma (cuando el sistema solicita la ejecución de determinado módulo) este no podrá ser accedido debido a que no existe una ubicación específica, o bien, se encuentra bloqueada y con ella la información del usuario.

CARACTERÍSTICAS DE COMPORTAMIENTO

- Para asegurar su propagación, cuando el usuario solicita la apertura de un objeto en particular (carpeta, archivo y/o una aplicación ejecutable) el virus direcciona dicha solicitud hacia donde se encuentra su código base, por lo tanto, al ejecutarse nuevamente todos los dispositivos conectados serán infectados.
- Al ser un programa residente, este *software* no puede transmitirse hacia otros sistemas computacionales que están conectado a través de una red local y/o nodo; por lo tanto, su principal vía de propagación es a partir de los puertos USB y de los dispositivos allí conectados.
- Por directiva en su diseño, el virus informático de directorio no podrá adherirse a objetos que ya se encuentren previamente secuestrados por otro tipo de amenaza, para estos casos, el programa buscará el elemento inmediato adyacente que se encuentre disponible.

Este tipo de “virus” contiene la particularidad de que, independientemente de que otros *softwares* del tipo antivirus puedan eliminar sus copias, su código base se mantiene intacto pues, teóricamente, no es malicioso sino hasta que comienza la propagación hacia múltiples objetos.

Existen programas tales como “*CHKDSK.EXE*” [59] capaces de reparar ciertos módulos, directorios, índices e incluso diagnosticar zonas del plato magnetizable que están próximas de deteriorarse; esencialmente este programa es el que pudiera restaurar aquellas áreas afectadas e incluso restablecer las rutas necesarias para recuperar el acceso a las direcciones donde la información del usuario está establecida [95].

VIRUS POLIFÓRMICO

Se le llama así por su capacidad progresiva para alterar su estructura lógica (patrón de líneas programables) con el fin de no ser detectado como amenaza; dichos cambios son visibles a partir de la infección del primer objeto, el segundo tendrá una estructura diferentes y así consecutivamente. Los cambios realizados por el *software* sólo afectan los patrones identificables por los motores de búsqueda de los programas “antivirus”, manteniendo así el código fuente intacto y aislado de procesos de análisis [29].

CARACTERÍSTICAS DE COMPORTAMIENTO

- Se encarga de infectar y destruir por igual objetos pertenecientes al usuario y/o SO, siempre y cuando estos se encuentren en el mismo directorio que la amenaza.
- Para poder propagarse de forma local en el SO, se almacena en una localidad temporal, espera a que el usuario solicite un segundo directorio y procede a alterar el primer objeto que sea visible. Su proceso infeccioso, a partir de este punto, no necesita de mayor intervención por el usuario en dicho directorio.
- Utilizan medios de encriptación de algoritmo, es decir, cuando se intenta eliminar su contenido (asumiendo que ya ha sido identificado como programa tipo “virus”) este solicitará una clave de acceso y, al no poseerla, el objeto será omitido de la desinfección.
- Algunas variantes obligan al SO a instalar y desinstalar los controladores (firma digital) para los dispositivos externos. El objetivo principal de realizar esta rutina es que, una vez desinstalados, los controladores serán “actualizados” por la amenaza y, de forma automática e inadvertida, el algoritmo fuente del *software* será transmitido a todas aquellas localidades posibles, típicamente, memorias digitales, arreglos de DDE externo y/o cualquier otro dispositivo de interfaz USB.
- Su condición de polimorfismo es exclusivamente local y no hay evidencia que sugiera que dichos programas pueden enviarse a través de la red por medios autónomos, solamente a partir de la acción directa del usuario (por ejemplo: adjuntando un objeto infectado y enviarlo a través de un servidor de correo electrónico).

- Algunas variantes pueden tomar posesión de todo un volumen, es decir, el usuario ya no es más el propietario de su información y, con dichos privilegios, el código vírico puede eliminar elementos según lo considere su programación.

El motor de búsqueda de algunos antivirus no trabaja exactamente a partir de la detección de código malicioso, sino de forma inversa, es decir, la **base de datos** que se actualiza de forma constante en realidad es un compendio de extensiones, cabeceras y contenidos de las nuevas versiones de archivos que los *softwares* “benignos” y legítimos utilizan para interactuar con el usuario y el SO; cuando un archivo no puede ser identificado dentro de esta “librería” entonces es marcado como infección y se procede a su respectiva eliminación y/o (de ser posible) desinfección.

Otro tipo de motor de búsqueda es aquel que funciona a partir de la detección de patrones repetidos en diferentes localidades, es decir, **patrones de algoritmo recursivos**; dicha característica resulta ineficaz en contra el *software* polifórmico estudiado debido a que, precisamente, todos sus patrones consecutivos son diferentes.

VIRUS “HOAX”

Se define como el tipo de *software* no malicioso en algoritmo pero fraudulento en operación transmitido a partir de servidores de correo electrónico. El programa “hoax” es un archivo cuya finalidad es la de generar mensajes de alerta sobre la presencia de “amenazas” que han secuestrado el equipo huésped; la realidad es que dichos “supuestos objetos infectados” en realidad conforman elementos fundamentales e irremplazables del SO únicos para su inicio, funcionamiento y operación.

CARACTERÍSTICAS DE COMPORTAMIENTO

- Dependiendo de su diseño de interfaz gráfica, pueden colocar al usuario en un estado de alerta en el que, mediante una serie de instrucciones manuales, este sea capaz de eliminar las “amenazas” que atentan contra el equipo.
- Debido a su algoritmo, este *software* es capaz de reproducir un ambiente tal en el que un “contacto” asociado a una cuenta de correo electrónico usurpada aparezca como el que ha enviado dicho objeto tal y como si se tratara de un mensaje

cualquiera, un segundo usuario procede entonces a abrir el contenido y, de esa forma, se completa el proceso infeccioso.

- Promueve en el usuario la necesidad inmediata de difundirlo a través de múltiples medios hacia sus diferentes contactos, siendo el correo electrónico la principal vía de transmisión para dicho *software*.
- Suele utilizar logotipos, emblemas y/o frases de marcas pertenecientes a empresas registradas para infundir en el usuario un estado de confianza y seguridad.

Las aplicaciones “hoax” no son detectables por los sistemas de antivirus como tal, pues, debido a su diseño, estos no son considerados como amenazas ya que todas las actividades destructivas son ejecutadas por el usuario; es posible establecer entonces que estos no son residentes en memoria, SO y/o DDE, sino de los nodos de red que interactúa con los elementos mencionados.

El objetivo real de estos dispositivos se basa en la destrucción o modificación de datos del SO de forma manual, con una marcada tendencia para promover distintos mensajes, típicamente, con fines lucrativos (publicidad) y destructivos del SO. Debido a su relevancia para el caso estudio presentado, es aquel cuya presencia no interfiere de forma alguna en la aplicación de métodos de extracción de datos, así como en los respectivos niveles de integridad obtenidos [97].

MÉTODOS DE DESINFECCIÓN

Se define como el compendio de tecnologías y procedimientos lógico-virtuales propios de un sistema “antivirus” que tienen lugar en un SO, las cuales, permiten la remoción y/o eliminación segura de *softwares* ajenos, infecciosos, maliciosos e inestables tales que alteren la dinámica de procesos normales de un objeto cualesquiera atentado contra el contenido del mismo en un momento determinado. Dicho “compendio” estará orientado siempre a procurar la estructura original de objeto infectado a fin de no causan daños colaterales.

De forma general, **el método heurística** es el principal encargado del proceso de desinfección, motor de búsqueda y detección de amenazas existente; sus distintas variantes conforman en sí el conjunto de métodos aquí estudiados, las cuales a su vez son [13]:

Heurística:

Es la capacidad para detectar algoritmos víricos que no se tienen originalmente contemplados en la base de datos principal del programa. Consiste en la comparación exhaustiva y minuciosa de la similitud entre un código plenamente identificado como “virus” en contra de otro desconocido, de definirse que dichos códigos son convergentes, el objeto es marcado como amenaza.

Heurística genérica:

Consiste en la identificación de firmas digitales genéricas y código interno compilado cuyas instrucciones sean consistentes con aquellas identificadas como amenazas.

Heurística pasiva:

Proceso, en una primera etapa, de observación y evaluación del comportamiento de un objeto seleccionado por un tiempo limitado, de determinarse una actividad anómala tales como funciones cíclicas y/o reiteradas, se procede entonces a marcar al objeto como amenaza.

Heurística activa:

Proceso de alto consumo de recursos, consiste en el monitoreo permanente de un objeto determinado durante sus etapas de inicio, interacción (esto implica que también dichos objetos secundarios son analizados), operación y cierre para, en función de los resultados obtenidos, determinar si su naturaleza es o no dañina para el SO.

Cualquier modalidad de heurística tiene la capacidad de eliminar archivos de forma autónoma, sin embargo, dependiendo del programa antivirus y de la configuración que el usuario disponga, alguna de las modalidades siempre será la predominante.

DESCRIPCIÓN DEL PROCESO DE REPARACIÓN

En esta sección se estudiará el proceso de restauración (mediante la utilización de *software* antivirus) de los elementos enumerados del 6 al 14 pertenecientes a la tabla 23 del presente capitulado. Este desarrollo tiene el fin de exponer el conjunto de daños lógicos en el DDE,

SO e información asociada a estos por causa de la ejecución de programas víricos, así mismo, se expondrán los métodos apropiados y se mostrarán los resultados obtenidos correspondientes.

Las distintas variedades de *software* malicioso expuesto, pertenecientes a la clasificación propuesta, fueron encontradas e identificadas operando bajo un entorno controlado de SO en una triada de diferentes muestras de DDE.

Dado que el objetivo particular de este apartado es el de ejemplificar y mostrar los daños lógicos y sus posibles métodos de solución para recuperar la información contenida, se utilizará la ejecución del *software* “antivirus” como el método universal de desinfección y eliminación de amenazas, mas no como uno de recuperación de datos.

Sin embargo, los comportamientos y estragos producidos por dichos tipos de programas citados conformarán un marco de datos significativo, fundamental e imprescindible para los fines del proyecto desarrollado, pues, el *software* de diseño “FERCUVILL V5.0” planteará tecnologías y medidas preventivas que resguarden, procuren y mantengan la integridad de la información en el DDE, así como de sus elementos estructurales físicos y lógicos.

Atendiendo a lo expuesto en el párrafo anterior, los datos medulares de interés estarán guiados por los siguientes campos:

- 1. Modificación de las propiedades de acceso a archivos y directorios contenedores.**
- 2. Principales vías de propagación primarias y secundarias utilizadas por las categorías de virus informáticos estudiados.**
- 3. Deterioro del contenido sustancial de los archivos creados por el usuario.**
- 4. Métodos de bloqueo del acceso al SO.**

A continuación, en la tabla 24, se proporcionan los datos de placa e información de disco (s) lógico (s) asociados a cada DDE anfitrión:

MARCA	MODELO	CAPACIDAD	VOLÚMENES LÓGICOS
A) SEAGATE.	ST3500413AS.	500 GB.	DISCO "C:".
B) WESTERN DIGITAL.	WD1600AAJS.	500 GB.	DISCO "G:".
C) MAXTOR.	5T020H2.	20.4 GB.	DISCOS "F:","W:".

Tabla 24. Datos de placa del conjunto de unidades de DDE utilizados para el estudio de daños lógicos a causa de *softwares* identificados del tipo "virus informático".

OBSERVACIONES PRELIMINARES

- Para el caso de los objetos A) y B) de la tabla 24, nótese que sólo existe un volumen/disco lógico identificado, por ello, debe de asumirse que estas particiones son primarias y, por lo tanto, contienen un único SO principal. En tanto que para el objeto C) se especifica que el volumen "F:" contiene al SO, mientras que el "W:" es una partición de datos.
- No debe de entenderse como regla general que, a mayor capacidad de almacenamiento le corresponde una mayor cantidad de volúmenes lógicos, dicha característica es opcional y configurable por el usuario.
- Los elementos A) y B) mencionados en la tabla 24 están ejecutándose bajo un SO base Windows [99] con una arquitectura de 64 bits, en tanto que C) opera en 32 bits [47, 70].
- Los datos del conjunto de DDE y de SO proporcionados son citados exclusivamente como referencia. Independientemente de las corporaciones encargadas de fabricar dichos dispositivos, los *softwares* maliciosos siempre intentarán vulnerar, indistintamente, cualquier medio de almacenamiento de datos, sin importar, cuan complejos, responsables y sofisticados sean en su diseño.

DISTRIBUCIÓN FÍSICA DE LAS INFECCIONES

En función de los datos presentados en las tablas 23 y 24, respectivamente y, a través de la utilización de *software* de antivirus ofertado por la **Universidad Nacional Autónoma de**

México [93], se genera la tabla 25, en la cual, se muestra la organización e identificación de las amenazas de acuerdo a cada DDE y volumen lógico analizado

DISCO FÍSICO	DISCOS LÓGICOS	AMENAZAS IDENTIFICADAS
ST3500413AS.	DISCO "C:".	<ul style="list-style-type: none"> • GUSANO. • MACRO BLT. • VIRUS "HOAX".
WD1600AAJS.	DISCO "G:".	<ul style="list-style-type: none"> • VIRUS DE PROGRAMA. • VIRUS DE INICIO. • VIRUS DE DIRECTORIO.
5T020H2.	DISCO "F:".	<ul style="list-style-type: none"> • CABALLO DE TROYA.
5T020H2.	DISCO "W:".	<ul style="list-style-type: none"> • VIRUS "ERS". • VIRUS POLIFÓRMICO.

Tabla 25. Distribución física y lógica de los códigos maliciosos en cada DDE anfitrión analizado.

PROCEDIMIENTO

De forma genérica, la reparación para este tipo de daños es, típicamente, semi-automatizada y mediante la utilización de *software* antivirus de acción general instalado en un equipo computacional externo con un SO independiente; solamente para amenazas específicas se deben de emplear herramientas igualmente especializadas en su diseño.

La configuración general de acción de los *softwares* antivirus está regida por el siguiente orden, de no cumplirse con el primero se ejecutará el segundo de forma automática:

1. Una vez lograda la identificación plena del código malicioso, proceder a aplicar un método de desinfección (eliminación del algoritmo foráneo y restablecimiento del código original del objeto afectado).
2. Cuando los métodos de desinfección aplicados sean infructíferos, proceder a aplicar un método de borrado completo (el objeto secuestrado y el algoritmo vírico son destruidos) a fin de evitar futuras infecciones en otros objetos.

El proceso de desinfección no es agresivo para los elementos del SO, en tanto que todo proceso de eliminación forzada y/o de borrado completo si lo es, por ello, este último es implementado sólo como último recurso y siempre con el consentimiento y conocimiento del usuario.

A continuación, se procede a realizar la descripción de las acciones del *software* “antivirus” para, posteriormente, analizar sus alcances y resultados obtenidos.

1. Ejecutar el programa, este inmediatamente guardará en memoria el conjunto de herramientas de detección, desinfección y eliminación de objetos necesarias.
2. Acceder a la consola de operaciones, también conocido como “menú principal”.
3. Definir los parámetros de operación, tales como: dirección del objeto a analizar (esta dirección puede contemplar: una partición completa, directorios y/o un archivo aislado), tipo de análisis (desinfección y/o eliminación) y recursos informáticos para la operación.
4. Iniciar el proceso, observar en pantalla el porcentaje y progreso obtenidos. Algunos sistemas de antivirus contabilizan las amenazas detectadas y enlistan sus identificadores (nombres).
5. Una vez concluidos todos los procedimientos de desinfección y eliminación seleccionados, reiniciar el equipo de cómputo para que el DDE y el SO se adapten a los cambios realizados.
6. Observar y comprobar las modificaciones ejecutadas por el programa “antivirus”, preferentemente, mediante la utilización del *software* “*explorer.exe*” para evaluar la disponibilidad de la información almacenada.

De forma opcional y, dependiendo del tipo de amenaza, es una práctica común el ejecutar un segundo análisis de antivirus sobre el objeto original, esto tiene lugar debido a que en ciertas ocasiones los elementos víricos que son eliminados constituyen solamente la copia y no así el archivo fuente del algoritmo infeccioso; un segundo análisis podría implicar el destruir y/o desinfectar la fuente y no solamente las copias genéricas del mismo.

Las indicaciones anteriores fueron aplicadas a cada uno de los discos anfitriones de forma individual. Así mismo, los parámetros de operación, tipos de análisis y resultados obtenidos se encuentran plasmados en la tabla 26 como se muestra a continuación:

VOLUMEN	PARÁMETROS DEL ANÁLISIS	TIPO DE ANÁLISIS	RESULTADOS DE LA DESINFECCIÓN	CALIDAD DE LA INFORMACIÓN
DISCO “C:”.	COMPLETO.	DESINFECCIÓN.	EXITOSA.	ÍNTEGRA.
DISCO “G:”.	COMPLETO.	DESINFECCIÓN Y ELIMINACIÓN.	PARCIAL.	INCONCLUSA.
DISCO “F:”.	COMPLETO.	ELIMINACIÓN.	EXITOSA.	DESCONOCIDA.
DISCO “W:”.	COMPLETO.	ELIMINACIÓN.	PARCIAL.	DESCONOCIDA.

Tabla 26. Aplicación de métodos de desinfección y eliminación de *software* vírico; obtención de resultados.

ANÁLISIS Y RESULTADOS DE LOS OBJETOS INTERVENIDOS.

En este apartado se estudiará la relación que existe entre los valores obtenidos a partir de la aplicación de distintos métodos de desinfección en contra de la integridad de la información misma y, según corresponda en cada caso, mencionar aquellas condiciones específicas que afectaron/afectan directa e indirectamente a la misma en su composición y/o edición.

Disco lógico “C:”

- El DDE analizado fue removido del equipo de cómputo original para aplicarle los procesos de análisis y eliminación de amenazas correspondientes.
- Se ejecutó un análisis completo del volumen pues, debido a la clasificación a la que pertenecen el conjunto de amenazas reportadas, los código infecciosos ya se encontraban residentes en diferentes directorios del SO.
- Mediante la inspección física y utilización de *software*, se observó que el DDE afectado sostenía altos índices de temperatura por encima de sus valores nominales de operación, lo cual, es consistente con un tipo de daño lógico estudiado (acción del virus tipo “WRM”).
- Múltiples copias de código malicioso fueron encontradas en carpetas exclusivas del SO para albergar *software* registrado utilizado para la edición de texto, sin embargo y puesto que la versión de la variante infecciosa no lo ejecutaba, la información producida por los programas no se encuentra corrupta.
- Todas las fuentes de código vírico fueron detectadas y eliminadas de forma automática, sin estragos identificables a la información contenida en el volumen.
- La visualización y extracción de los datos fue llevada a cabo por medio de la utilización del explorador de archivos.

Disco lógico “G:”

- El DDE analizado fue removido del equipo de cómputo original para aplicarle los procesos de análisis y eliminación de amenazas correspondientes.
- La detección, a través del *software* “*diskmgmt.msc*”, del volumen lógico fue inicialmente exitosa, en ese momento se le aplicó un análisis de antivirus y se logró desinfectar la variante modificada: “virus de programa”, en tanto que las variantes de: “virus de inicio” y de “directorio” fueron detectadas pero incapaces de ser eliminadas.
- Posterior al primer proceso de desinfección y a un reinicio del equipo de cómputo utilizado, el DDE mostró un mensaje de error en pantalla referente a un fallo en el dispositivo de E/S, por lo tanto el acceso estaba restringido.

- Mediante la comprobación por *software* se determinó que los primeros 2048 B del DDE infectado se encontraban marcados como defectuosos/bloqueados (incluido el sector RAP), por tal motivo, el acceso al contenido de la tabla de particiones no fue posible y, con ello, la recuperación de la información allí contenida.

Disco lógico “F:”

- El DDE analizado fue removido del equipo de cómputo original para aplicarle los procesos de análisis y eliminación de amenazas correspondientes.
- El proceso de desinfección logró eliminar eficientemente las amenazas detectadas, el SO perteneciente a ese DDE sufrió deterioro virtual debido a que la mayoría de estas copias se encontraban alojadas en el directorio principal del sistema. Sin embargo, las carpetas contenedores de la información del usuario se encontraban intactas.
- Completados todos los procedimientos de eliminación de amenazas, se procedió a realizar un reinicio del sistema para verificar el estado y calidad de la información almacenada.
- La detección del DDE ante el BIOS y del volumen asociado ante el *software* “*explorer.exe*” fueron logradas satisfactoriamente.
- Mediante la utilización del explorador de archivos, fue posible observar la información contenida y organizada a manera de carpetas; sin embargo, las propiedades básicas de lectura se encontraban deshabilitadas y, en adición, no se contaban con los permisos administrativos suficientes para realizar la extracción directa. Este par de estragos lógicos son remanentes característicos de infecciones por programas del tipo “troyano”.
- La información, pese a estar presente y localizada en la partición desinfectada, no es accesible, por lo tanto, la integridad de la misma no son comprobables (**Véase el “CASO DE ESTUDIO 2” con “FERCUVILL V5.0”**).

Disco lógico “W:”

- De igual forma para este y, debido a que su SO original ya estaba mermado en su estructura, al volumen se le aplicaron los procesos de análisis y eliminación de amenazas correspondientes.
- Las infecciones por virus del tipo “troyano” sólo afectaron la partición primaria, sin embargo esta, al ser del tipo secundaria y utilizada como de almacenamiento de datos, se encontraba intervenida por diferentes variantes identificadas de los virus tipo: ERS y polifórmico.
- Se le aplicó un proceso de análisis completo configurado con eliminación forzada de elementos infectados, pues, por la naturaleza del código malicioso, la información podría ser borrada de forma aleatoria; en términos de recuperación de datos, esto representaría una pérdida definitiva, por tanto, esto no es permisible bajo ninguna circunstancia. Para el caso particular del objeto analizado, la fuente principal de la infección estaba propagada en el directorio de mayor tamaño.
- El análisis aplicado eliminó eficientemente las variantes identificadas de: “virus ERS”, sin embargo, dicho análisis mostró un nuevo *software* malicioso que, previamente, nunca fue identificado; este comportamiento corresponde al virus polifórmico; llegado a este punto es necesario detener todo proceso de desinfección pues, de continuar, el virus continuaría modificándose y adoptándose para evitar su eliminación, o bien, alcanzaría un estado en el que el mismo sistema “antivirus” sería incapaz de detectarlo.
- El virus de tipo polifórmico se encuentra en la raíz de la partición, es decir, directamente en “W:”, por ello, no es recomendable acceder al directorio pues, de acuerdo a sus características de operación, el hecho de solicitar la apertura de un archivo cualesquiera infectaría a todos los adyacentes en dicha dirección, comprometiéndolos inmediatamente. Puesto que la información a recuperar aún está bajo la influencia de *softwares* maliciosos y, en edición, no se puede obtener los registros de los daños producidos por la primera amenaza, los índices de calidad siguen siendo ambiguos.

CONCLUSIONES PARCIALES

En esta sección se analizaron el conjunto de condiciones lógicas internas y externas al objeto estudiado: el DDE. Así mismo, se implementaron los distintos métodos correspondientes a cada tipo de daño mencionado en función de una metodología que implica la utilización, principalmente, de *software* especializado.

Es necesario establecer que, aunque se logre una reparación (restauración de acceso a objetos y/o desinfección de los mismos) con índices aceptables, la información no necesariamente se encontrará en óptimas condiciones tanto para su edición como para su extracción, esto es, ya que un daño lógico, como se observó en las diferentes etapas, tiene causas multifactoriales y depende igualmente del momento y evento que lo definieron inicialmente y, en adición, el origen del mismo puede ser igualmente por condiciones de *software* y/o por *hardware* (estructura cuyos daños y posibles métodos parciales de reparación serán analizados y expuestos a continuación) conjuntos, lo cual lo torna aún más complejo.

Los eventos externos son igualmente determinantes que los internos, establecer las dinámicas de operación y métodos de solución es un aporte crítico para lograr mejores condiciones y aumentar las probabilidades de una recuperación de datos efectiva.

Una tendencia destacada en las “características de operación” de los tipos de virus informáticos analizados durante el presente estudio fue aquella en la que, a su vez, se indica un contagio consistente y considerable a través del uso de dispositivos compatibles con la interfaz USB: memorias digitales y arreglos de DDE externos.

Los resultados finales de los procedimientos de recuperación de datos aplicados a los objetos A), B) y C) de la tabla 24, así como el objeto de la figura 31 están plasmados, respectivamente, en los casos de estudios indicados y, correspondientes al capítulo del *software* diseñado (ver página 194). En la tabla 27 se condensan las estadísticas proporcionadas por la empresa Microsoft [99, 56] referentes a la necesidad e importancia del contar con protección activa ante la última condición lógica descrita.

DESCRIPCIÓN	DATOS
1. Porcentaje de equipos registrados (detectados) a nivel mundial los cuales no cuentan con un <i>software</i> antivirus residente, o bien, se encuentra desactualizado.	24%
2. Propensión de un sistema computacional sin protección informática a contraer <i>software</i> malicioso tipo “virus” en comparación a otro que si la posee.	550%
3. Sistemas de cómputo desinfectados en el segundo semestre del año 2012 del <i>software</i> “Onescan”, el cual brindaba una protección falsa, aumentando la tendencia de ataques informáticos a causa de programas maliciosos.	3 millones.

Tabla 27. Tendencias, comparaciones y estadísticas de sistemas computacionales sin protección antivirus y/o desactualizada.

2.2 CORRUPCIONES MECÁNICAS Y POSIBLES MÉTODOS DE REPARACIÓN

De igual forma que la estructura lógica, la estructura mecánica fue estudiada en el capítulo anterior y, a su vez, definida como aquella que se encarga de relacionar todos los principios físicos (señales eléctricas y electrónicas, movimientos, soporte, herrajes y hasta interfaz de conexión) suficientes que permitan a la estructura lógica desempeñar sus operaciones y funciones virtuales.

En este apartado se estudiarán el tipo de condiciones mecánicas críticas tales que puedan: impedir la extracción de datos (eliminación del medio de comunicación), suprimir flujo

eléctrico para la energización de elementos y/o (potencialmente) destruir por completo el medio físico en el que la información existe.

Una característica única de esta estructura es, precisamente, que prácticamente todos sus fallos pueden ser identificables mediante una inspección visual y el uso de herramientas, en tanto que, una mínima a través del uso de *software*, pues, no es posible ejecutar programas cuando la estructura mecánica colapsa.

Pese a que su estudio se ha dividido, estas estructuras no son exclusivas la una de la otra. El funcionamiento óptimo de una afectará positiva o negativamente el comportamiento de la otra.

Se define como **daño mecánico** a toda aquella condición de índole física y de *hardware* que impida el acceso a la información almacenada de forma parcial y/o total a través de la perturbación de los medios físicos encargados de procurar los procesos de lectura y escritura de datos llevados a cabo tanto interna como externamente por los dispositivos implicados [60].

Al igual que en el caso de la estructura lógica, se expondrán las problemáticas más comunes así como las técnicas propias para cada caso, indicando la descripción de los procesos aplicados y los resultados parciales/totales correspondiente de acuerdo al método aplicado.

La definición de “daño mecánico” puede ser extendida hasta el concepto de **fallo por hardware**, el cual a su vez se define como todo aquel estado físico adverso de carácter parcial, total, temporal y/o permanente en el cual se establecen condiciones como: deterioro y desgaste de materiales, dispositivos precarios y/o arreglos dinámicos completos inestables, **deterioro directo de la estructura lógica** y/o cualquier otro tal que sea capaz de comprometer la integridad del medio físico de almacenamiento de datos y, con ello, la calidad y existencia de la información allí contenida [4].

Aplicando la definición anterior al objeto de estudio analizado, un fallo por *hardware* estará presente en el DDE cuando se establezcan alteraciones en la arquitectura física de las siguientes estructuras:

1. Módulo *firmware* (tanto el almacenado en la TCI como en los platos magnetizables).
2. Circuitos eléctrico-electrónicos: el conjunto TCI.
3. Actuador degradado/desgastado (cabeza y cabezal completos).
4. Platos magnetizables (fisuras, fracturas y marcas circulares).
5. Cubierta y carcasa (filtraciones y alteraciones del medio).
6. Motor (rodamientos del tipo BB y FDB).

Las alteraciones producidas en las estructuras anteriores, fundamentalmente, pueden ser ocasionadas por las siguientes circunstancias:

1. Perturbaciones de naturaleza eléctrica en las interfaces de conexión del dispositivo de almacenamiento.
2. Impactos dinámicos y envejecimiento del material en las estructuras de soporte.
3. Ausencia de elementos de supresión/control eléctricos.
4. Por *software*, es decir, mediante la actualización errónea de elementos relacionados con el módulo *firmware*.
5. Alineación vertical fuera de rango, esto es, cuando el motor de eje central se enfrenta a vibraciones mecánicas por un desajuste ortogonal a su base y rodamientos.
6. Alteraciones en los circuitos de control (TCI) por causa de *software* inestable y/o malicioso.
7. Ambientales, es decir, por el medio físico tales como: humedad, temperatura e impurezas.

Los procedimientos y respectivos métodos de solución parciales y/o totales (igualmente temporales) expuestos se realizarán a través de la implementación de herramientas mecánicas básicas, en tanto que, los resultados (virtuales) referentes a la recuperación de datos serán comprobados a través de la utilización de *software* de diseño y/o nativos del SO utilizado asociados a las extensiones de los archivos.

Debido a la incidencia, relevancia como caso de estudio, complejidad y procedimientos implicados, para el presente proyecto de investigación, se analizarán exclusivamente aquellos daños mecánicos referentes a:

- A) CASO 1: MOTOR DE EJE CENTRAL.
- B) CASO 2: SECTORES CON DAÑO FÍSICO.
- C) CASO REPRESENTATIVO 3: PATRÓN DE RAYADO PERMANENTE APLICADO POR EL CABEZAL DIRECTAMENTE AL PLATO MAGNETIZABLE.

El inciso C) es resaltado debido a que atiende directamente el impedimento total y de carácter permanente que engloba una recuperación de datos a nivel físico y de *hardware*.

2.2.1 CASO 1: MOTOR DE EJE CENTRAL

De acuerdo a lo estudiado en el capítulo anterior, el DDE utiliza un impulso dinámico para generar un movimiento circular constante, el cual, es soportado en un eje vertical fuertemente asido a la base de la carcasa. Dicho elemento puede ser susceptible de perturbaciones, las cuales, comprometan su funcionamiento hasta tal grado en el que, aun cuando no se externen síntomas plenamente identificables, los elementos dependientes de este (discos rígidos y actuador) ya se encuentren ejecutando algún proceso destructivo del medio físico donde reside la información.

En este apartado se estudiarán aquel conjunto de condiciones bajo las cuales, al ser sometido, el motor de eje central experimentará un funcionamiento errático y, por lo tanto, un comportamiento intermitente. Dichos comportamientos son de carácter universal para el par de tipos estudiados: el BB y el FDB; estos se enlistan a continuación:

1. Producción de fricción mecánica entre los rodamientos del motor, la cual, es traducida en vibraciones directas causantes de un desajuste en la línea vertical descrita por el eje soportado en la carcasa.
2. Desgaste en el material fluido utilizado para proporcionar lubricación a los elementos móviles internos del dispositivo.

3. Presencia de desgaste de material, ya sea en el relacionado al soporte físicos de los platos magnetizables y/o al bobinado interno del motor; este último, a causa de valores de corriente y voltaje fuera de rango de los márgenes nominales de operación contemplados para su operación permanente.
4. Exposición a altas temperaturas durante las etapas de operación prolongada en estado permanente del elemento dinámico. Dichas condiciones son producidas por la precaria ventilación y/o la temperatura ambiente del medio de trabajo en el que se encuentre el DDE.
5. Desconexión súbita de la fuente de alimentación eléctrica proporcionada en los buses (interfaz) de alimentación. Dicha anomalía establece una relación de corto-circuito temporal, cuya presencia, altera físicamente la capacidad de operación del bobinado estructural. Existen situaciones en las que el corto-circuito se mantiene durante ciertas constantes de tiempo, la consecuencia directa entonces es la fundición del alambre magneto y la solidificación de los rodamientos, impidiendo así la rotación del elemento estudiado.
6. Cambio de las propiedades físicas del fluido viscoso utilizado como lubricante en los rodamientos. Dicho fenómeno impide una rotación a velocidad angular constante, produciendo con ello que el actuador completo sea incapaz de sincronizar el cilindro, la pista y el sector solicitados.

Así mismo, las condiciones mecánicas previamente expuestas producirán, principalmente, un par de anomalías, las cuales, suprimen de forma inmediata toda relación lógica del DDE con el *software* BIOS y, con ello, la información allí contenida:

1. Incapacidad total de establecer protocolos de comunicación digital y analógica entre la TCI del DDE con el módulo BIOS.
2. Ante un evento de “rotor bloqueado” y, en un intento por romper el torque inicial, la alimentación eléctrica principal producirá una corriente destructiva que fundirá todo elemento interconectado a esta. Exclusivamente el controlador VCM y/o los diodos de protección son los elementos fijos que podría prevenir dicho comportamiento.

De forma universal, la solución primaria para resolver impedimentos de lectura (y por tanto de escritura) de datos en el DDE relacionados al motor de eje central es, por medio de la

reparación temporal del mismo y/o su reemplazo, todo esto, mediante el uso de herramientas especializadas que permitan la colocación de uno con condiciones óptimas de operación, o bien, mediante la utilización de técnicas externas temporales cuya presencia permita la extracción de información de forma ininterrumpida.

DESCRIPCIÓN DEL PROCESO DE REPARACIÓN

Se observan, en la tabla 28, los datos de placa (y lógicos) para un DDE (figura 39) de tecnología identificada como FDB afectado, específicamente, en sus rodamientos a causa de una degradación de las propiedades físicas de viscosidad del fluido utilizado.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	TOSHIBA.
MODELO.	MK6025GAS.
DBL.	117210240 SECTORES.
INTERFAZ.	IDE.
CAPACIDAD DE ALMACENAMIENTO.	60 GB.
VOLÚMENES CONTENIDOS.	1 DISCO LÓGICO (UNIDAD "C:").

Tabla 28. Datos de placa para DDE con degradación del fluido viscoso presente en los rodamientos de motor de eje central.

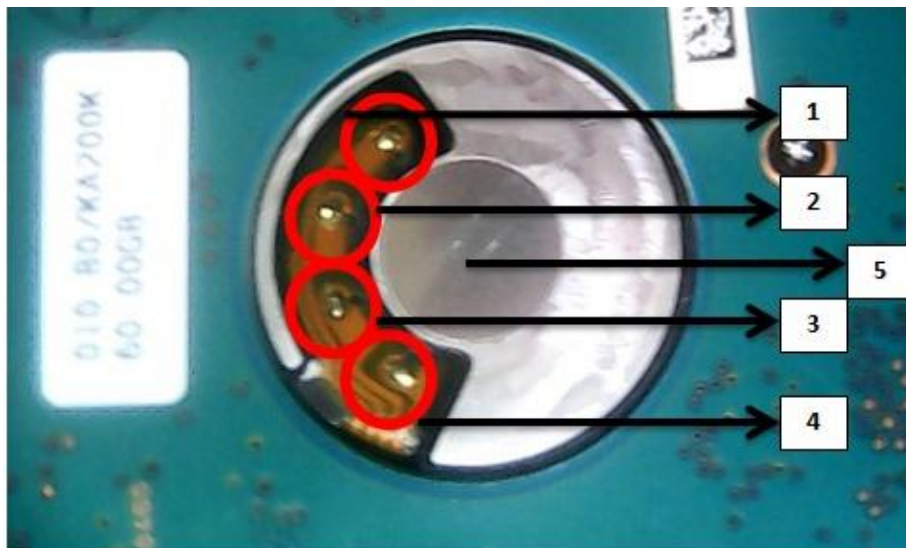


Figura 39. Visualización del motor de eje central con impedimento para girar debido al deterioro de las propiedades físicas del fluido viscoso.

A continuación, en la tabla 29, se muestran los elementos especificados en la figura 40, nótese la cercanía con la que los elementos se encuentran distribuidos, dicho evento es relevante al momento de aplicar calor, si bien la soldadura utilizada en este dispositivo tiene un alto punto de fusión [73] (menor a los 450°), no debe de ignorarse, o bien, se terminará fundiendo y haciendo contacto con sus consecutivos, con ello, el motor estará bajo una condición de corto-circuito y, de alimentarse eléctricamente, se fundirían los devanados internos.

ELEMENTO	DESCRIPCIÓN
1	FASE/PASO 1.
2	FASE/PASO 2.
3	FASE/PASO 3.
4	FASE/PASO 4.
5	EJE CENTRAL VERTICAL.

Tabla 29. Identificación de elementos externos y puntos de conexión para un motor de DDE.

Se determinó, mediante la aplicación de pruebas de estrés mecánico, que dicho DDE se encuentra afectado en sus rodamientos a causa de la solidificación en el líquido lubricante, esta condición impide la libre rotación del motor eléctrico y la extracción de datos correspondientes. De forma adicional, este DDE previamente no presentó síntomas de daños lógicos.

PROCEDIMIENTO

De forma exclusiva para este DDE (y basándose en su tecnología de rodamientos), la reparación será implementada a partir de la utilización de técnicas y herramientas externas no invasivas (aquellas que no impliquen la exposición directa de los elementos internos) cuya función será la de proveer, de forma temporal, un estado óptimo para la habilitación y restablecimiento del movimiento del motor y, con ello, restaurar la comunicación lógica en DDE.

Puesto que el objetivo principal reside en restituir la movilidad en los rodamientos sin alterar físicamente, tanto la TCI como los elementos adyacentes; el proceso de reparación

temporal efectuado consistirá en la aplicación forzada y dirigida de energía calorífica (por medio del aire) directa a la base del motor, y en específico, en el eje vertical que es en donde existe el fluido deteriorado.

El procedimiento aplicado pretende excitar dinámicamente las moléculas del lubricante a tal punto en el que se produzca un aumento en la fuerza de cohesión del mismo fluido y, de forma simultánea, una baja en la adhesión existente entre este último y el metal del eje.

La consecuencia directa será entonces que el lubricante fluirá momentáneamente en tanto se le continúe excitando con energía calorífica; permitiendo así el libre movimiento del motor y la subsecuente recuperación de datos a partir de la utilización de *software* especializado.

HERRAMIENTAS Y MATERIALES

Los elementos y equipos utilizados para realizar dicho procedimiento se enlistan a continuación:

1. **Pistola de aire caliente** con capacidad de proporcionar un flujo regulado y variación en los niveles de temperatura otorgados.
2. **Adaptadores y reguladores** tales que coincidan con el diámetro del eje al que se le aplicará el flujo de aire caliente, el cual, para este caso es de 6 milímetros.
3. **Papel tipo “aluminio”**, el cual, fungirá como un protector térmico de los elementos adyacentes a la base del motor, concentrándose así el calor solamente en la zona deseada.
4. **Sistema computacional externo**, el cual, provea del SO necesario para lograr identificar, ejecutar *software*, visualizar el volumen lógico y extraer el conjunto de información almacenada en la partición.

Una vez extraído el DDE dañado, es necesario seguir los siguientes pasos en el orden que se muestra a continuación, todo esto con el fin de ejecutar debidamente cada una de las acciones especificadas y recuperar la información contenida.

1. Colocar el DDE de tal forma que la parte anterior del mismo (es decir, en la que es visible la TCI) se muestre visible y accesible (figura 40):



Figura 40. Posicionamiento del DDE con la cara anterior expuesta.

2. Recubrir (incluso los bordes superiores e inferiores) con papel tipo “aluminio” toda aquella superficie que no se expondrá al calor aplicado (TCI completa), excepto la que contiene al eje vertical y los contactos del motor (figura 41).



Figura 41. Recubrimiento del DDE con papel tipo aluminio y exposición del área que contiene al motor.

Hasta este punto, el DDE se encontrará seguro de recibir un flujo de aire caliente en donde no se deba de aplicar; las consecuencias directas de ignorar la protección del papel tipo aluminio serían las siguientes:

- Deformación de los materiales plásticos y ondulaciones, las cuales, se traducen en fracturas (perceptibles e imperceptibles) de las pistas conductoras encargadas de establecer la alimentación eléctrica y/o comunicación bidireccional de datos lógicos).
- Fundición del conjunto de circuitos eléctrico-electrónicos de la TCI.
- Derretimiento de la soldadura, falsos contactos y coto-circuitos identificados por la unión de incorrecta de elementos (internos y externos a la carcasa).

Es necesario instalar el adaptador correspondiente para el diámetro correcto, como ya se mencionó anteriormente, para este caso es el de 6 milímetros. Dentro de las especificaciones del producto, el adaptador debe de soportar la temperatura a la que se someta durante el tiempo de calentamiento, de lo contrario, podría presentar deformaciones y, de forma involuntaria, re-direccionaría el flujo de aire caliente a una zona errónea. El adaptador (figura 42) utilizado para el procedimiento se muestra a continuación.



Figura 42. Adaptador de 6 milímetros para pistola de aire caliente.

3. **Instalar el adaptador en la salida principal de la pistola de aire caliente, asirlo firmemente para evitar filtraciones y pérdidas del flujo (figura 43).**



Figura 43. Instalación del adaptador y aseguramiento físico del mismo en contra de la pistola de aire caliente.

4. **Con la pistola y adaptador completos, ajustar la perilla de control de temperatura hasta un valor máximo de 370° y operar el equipo en vacío (sin calentar ningún objeto) por un lapso de 30 segundos; una vez alcanzado dicho valor, reducir por completo su funcionamiento (figura 44).**



Figura 44. Ajuste de temperatura y reposo de la pistola de aire caliente operada en vacío.

5. Posicionar el equipo térmico (y adaptador) de forma paralela a la base del eje vertical del DDE (figura 45), remover la cubierta protectora del motor.



Figura 45. Posicionamiento del DDE, pistola de aire caliente y adaptador colocados de forma paralela.

6. Una vez establecidos todos los elementos, energizar el equipo térmico y realizar movimientos a manera de pequeños círculos dispuestos en sentido anti-horario por un periodo de exposición igual a 10 segundos, posteriormente, repetir la operación pero con un sentido horario.
7. El periodo de exposición a la fuente de calor concentrada debe de estar de entre los 40 a los 60 segundos, finalizado este periodo, retirar y dejar reposar el material (evitar la fatiga y sobre-calentamiento). Posterior a este periodo, retirar la porción necesaria de papel tipo aluminio tal que permita conectar el DDE al equipo externo mediante la utilización de sus interfaces de datos y alimentación eléctrica. Una vez acopladas las conexiones físicas, energizar el dispositivo de almacenamiento y esperar el reconocimiento por parte del SO.
8. Una vez alcanzado un periodo de reposo de 10 segundos, proceder a repetir el paso 7, igualmente, hasta un periodo máximo de 60 segundos al mismo tiempo en el que el DDE se encuentra operando.

De realizarse correctamente los pasos anteriores y, que en adición, no exista un daño lógico determinante (daño en sector RAP y/o adyacentes, variantes de programas tipo “virus” que imposibiliten el acceso, copiado y/o manipulaciones en general de la información

almacenada) el lubricante de los rodamientos recuperará sus propiedades viscosas y permitirá el accionamiento del actuador, cabezal, deslizador, cabezas y SO necesarios para la visualización de los datos contenidos en el volumen.

Dado que el método expuesto es estrictamente temporal y provisional, la información debe de ser extraída, copiada y guarecida lo más rápido posible en alguna localidad independiente (típicamente un arreglo de DDE externo/portátil). Atendiendo este punto, el *software* de diseño “FERCUVILL V5.0” contempla un módulo de recuperación de información en equipos física y lógicamente inestables, el cual, fue aplicado a este objeto con resultados satisfactorios. (Ver el “CASO DE ESTUDIO 4” con “FERCUVILL V5.0”).

9. Una vez dentro del SO, ejecutar el *software* asociado a este para ejecutar el copiado de datos; dicha operación **no** puede ser completada mediante la utilización del explorador de archivos.

Normalmente, de ser ejecutados todos los pasos anteriores, el DDE se encontrará en condiciones tales que permitan la correcta movilidad de sus rodamientos y, por lo tanto, exista una sincronización propia entre los dispositivos mecánicos y los lógicos (digitales/virtuales) encargados de localizar y acceder a la información almacenada. A continuación, en la tabla 30, se muestra, de forma condensada, el conjunto de operaciones y resultados obtenidos a partir de la implementación del método de reparación expuesto.

ELEMENTO	TIPO DE DAÑO/CARACTERÍSTICAS	MÉTODO APLICADO	RESULTADOS
DEGRADACIÓN DE LA VISCOSIDAD EN LOS RODAMIENTOS	MECÁNICO, CON IMPOSIBILIDAD DEL MOTOR PARA GIRAR E INICIAR COMUNICACIÓN LÓGICA.	REPARACIÓN TEMPORAL MEDIANTE LA APLICACIÓN DE CALOR A LOS RODAMIENTOS.	OPERACIÓN EXITOSA. RECUPERACIÓN COMPLETA.

Tabla 30. Motor eléctrico y sus rodamientos, tipo de daño, método de solución y resultados.

CONCLUSIONES PARCIALES

En esta sección se analizó un DDE de rodamientos tipo FDB afectado en el motor de eje central por degradación en las propiedades viscosas del fluido lubricante; así mismo, se utilizaron herramientas externas para, mediante una excitación de energía calorífica externa, promover que el fluido recuperara momentáneamente sus propiedades físicas y permitiera el libre movimiento del motor instalado. Como complemento, el *software* de diseño “FERCUVILL V5.0” fue utilizado para realizar el proceso seguro de extracción de datos.

La solución expuesta no debe de ser considerada como universal y/o permanente, es decir, aunque la tecnología existente en cada caso (BB o FDB) en los rodamientos es la misma, tanto la organización, diseño, distribución, propiedades físicas (punto de fusión) y arreglos internos varían de acuerdo a cada fabricante y modelo específicos; como evento particular para este DDE, se observó que, en cuanto se le suprimió la aplicación de energía calorífica, el motor comenzó a experimentar nuevamente dificultades en su giro, por ello y durante la etapa de extracción, la excitación fue aplicada permanentemente. La lectura interna y escritura externa fueron ejecutadas correctamente.

2.2.2 CASO 2: SECTORES CON DAÑO FÍSICO

En el capítulo anterior se estableció el orden físico y lógico en el que la información es almacenada, si bien el “byte” es la mínima cantidad de información significativa para un sistema digital, el “sector” lo es igualmente para el DDE, **“es la mínima locación posible para almacenar un dato legible por un sistema computacional”**.

Cuando se menciona el término de **daño físico de un sector** debe de entenderse que dicho elemento se encuentra deteriorado, por condiciones internas y externas, en su superficie ubicada en el disco rígido y no será accesible por ningún medio de *hardware* y/o *software* disponible. En la práctica, cuando se menciona solamente el término de **daño en el sector**, típicamente, se refiere a aquella condición de naturaleza lógica en la que los dispositivos encargados de ejecutar las instrucciones de lectura y escritura son incapaces de acceder a dicha dirección, ya sea por bloqueo y/o por acción directa del módulo *firmware*.

A continuación, se enlistan las razones bajo las cuales se pueden presentar daños físicos en los sectores.

- a) Presencia de elementos externos (suciedad) en el deslizador y, en específico, en las cabezas.
- b) Marcas y/o humedad en la superficie de los platos producidas por la operación errónea (apertura del DDE) bajo un ambiente hostil.
- c) Desbalance en el motor de eje central, con lo cual, se produce un roce progresivo entre el deslizador y la superficie del plato.
- d) Deformaciones producidas en los discos rígidos por condiciones varias tales como: impactos físicos contundentes, deficiente colocación del DDE durante sus etapas de funcionamiento cuando este opera como interno y/o externo (colocado a 90 grados de la superficie de trabajo en lugar de mantenerlo a 180 grados) y/o aplicación de un movimiento brusco cuando el motor de eje central se encuentra energizado.

Los incisos b) y c) son los que presentan mayor incidencia, esto debido a que básicamente el usuario no cuenta con los conocimientos básicos de mantenimiento y cuidados necesarios, lo cual, contribuye a incrementar la gravedad y extensión del daño presentado.

PROCESO DE IDENTIFICACIÓN DE LA FALLA FÍSICA

Es posible definir la existencia de sectores dañados físicamente a partir de la manifestación de los siguientes síntomas a partir de la utilización de *software*. [102]:

1. **Error de lectura de disco.** Durante la etapa de reconocimiento del DDE por el *software* BIOS, reportarán mensajes de errores determinantes, específicamente, durante la fase de lectura (figura 46). Como caso particular, si el sector físico dañado es el RAP y/o sus inmediatos, se experimentarán las condiciones descritas en el caso de estudio presentado en la sección de fallas lógicas (ver tema 2.1.1).

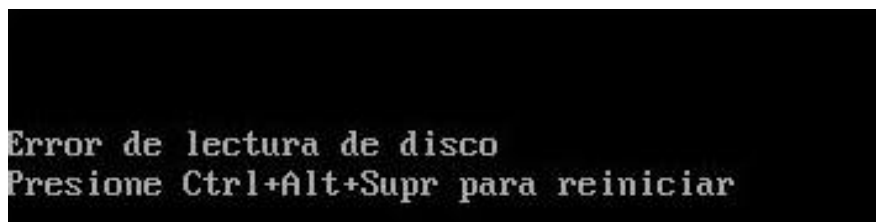


Figura 46. Visualización de mensajes de error para un DDE con sectores de inicio dañados físicamente.

2. **Error en la escritura demorada.** Existe una identificación por parte del SO a través de los *softwares* “*explorer.exe*” y “*diskmgmt.msc*”, pero al intentar acceder al volumen y a la información contenida se produce el error, el cual, indica un retardo en la escritura (figura 47). Este síntoma, de la misma forma, puede ser un problema combinado con una intermitencia de la alimentación eléctrica en la TCI hacia el motor.



Figura 47. Visualización del mensaje de error para una demora en los procesos de escritura de datos.

3. **Error por redundancia cíclica.** Existe una incapacidad del SO para leer/escribir datos en una determinada localidad (figura 48). El usuario es incapaz de visualizar el contenido del archivo y/o carpeta específicos y, al intentar copiarle, un mensaje de estado de error le es mostrado.

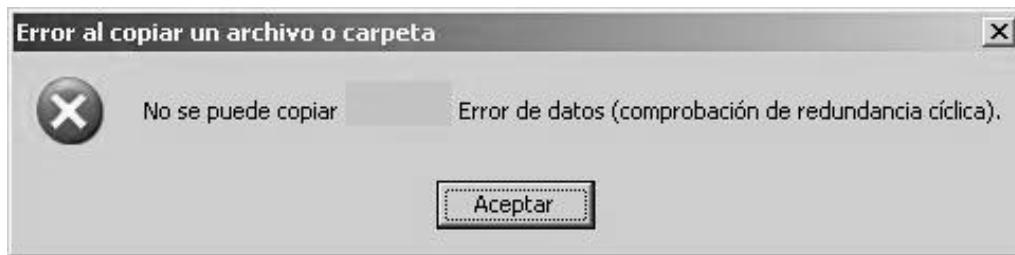


Figura 48. Visualización del mensaje en pantalla para un error de redundancia cíclica durante el proceso de copiado de información.

4. **Error de dispositivo, el objeto está dañado o ilegible:** Es aquel en el que existe una identificación del SO y del *software* “*explorer.exe*”, sin embargo, al intentar abrir el objeto (una partición), los procesos de ejecución de lectura de datos son incapaces de acceder al volumen especificado, por lo tanto, los datos allí son ilegibles por el sistema (figura 49).

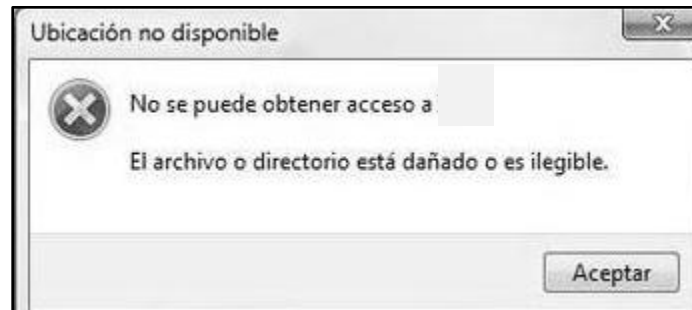


Figura 49. Visualización del mensaje de error durante el acceso a un volumen dañado.

La clasificación de errores mencionada anteriormente no es mutuamente excluyente, es decir, puede estar combinada con fallos lógicos, sin embargo, mediante la inspección física del objeto analizado es que es posible definir, en su mayoría, el tipo de daño predominante.

Se observa que, tanto para fallas lógicas como para mecánicas, el mensaje de error establecido en las figuras 23 y 46 converge; sin embargo, y en adición para la falla mecánica, es posible observar dicho error combinado con sonidos y/o golpes agudos internos en la carcasa, estos a su vez, son producidos por los movimientos del cabezal, el cual, intenta de forma recursiva la lectura de la zona dañada sin conseguirlo. Exponer al DDE a movimientos agresivos, repetitivos y prolongados de esta naturaleza no sólo agravará el problema, sino que puede producir un contacto físico de mayor magnitud y, con ello, una extensión mayor de daño físico.

DESCRIPCIÓN DEL PROCESO DE REPARACIÓN

A continuación, en la tabla 31, se observan los datos de placa (y lógicos) para una unidad de DDE (figura 50) que presenta sectores físicamente dañados en el volumen principal.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	WESTERN DIGITAL.
MODELO.	WD100BB-60BCB0.
DBL.	19541088 SECTORES.
INTERFAZ	IDE.
CAPACIDAD DE ALMACENAMIENTO.	10 GB.
VOLÚMENES CONTENIDOS.	2 DISCOS LÓGICOS (UNIDADES "C:", "Q:")

Tabla 31. Datos de placa para DDE con sectores dañados físicamente.

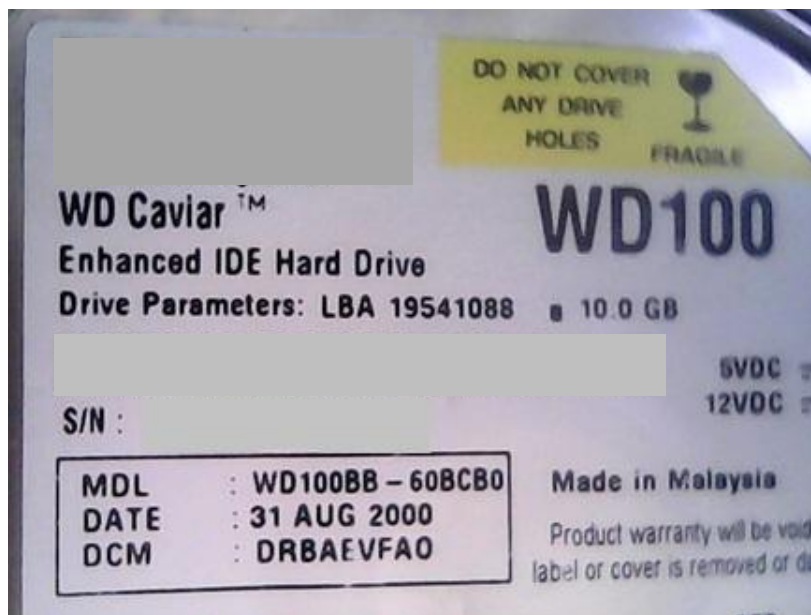


Figura 50. Datos de placa para un DDE con sectores físicamente dañados.

Un aspecto importante a considerar en particular para este DDE es la fecha de fabricación del mismo. Un DDE que ha experimentado un considerable tiempo de trabajo prolongado definitivamente será más propenso a sufrir un daño físico, lógico y/o la combinación de ambos a causa de un desgaste generalizado en sus materiales de construcción.

PROCEDIMIENTO

El DDE de la figura anterior, mediante la inspección y pruebas físicas/lógicas aplicadas, mostró como resultados los siguientes comportamientos al conectarlo a su sistema computacional original:

1. Presentó, durante la etapa de reconocimiento ante el módulo BIOS, dificultades para su identificación lógica y, como complemento, el tiempo de descarga del SO en memoria fue inusualmente largo.
2. Una vez iniciado el SO, de forma intermitente pero plenamente identificable, el actuador presenta golpeteos cuando se intenta acceder al volumen secundario a través de la utilización del explorador de archivos.
3. Se presentaron los errores de: “**redundancia cíclica**” y “**objeto dañado o ilegible**” estudiados en 3) y 4) respectivamente de la sección anterior. Existió una incapacidad del sistema para mostrar el contenido de la información.
4. Se ejecutó un segundo intento para acceder al DDE mediante la utilización provisional de un sistema computacional externo, como consecuencia de esto y en adición a los síntomas del punto anterior, el dispositivo incrementó visiblemente su temperatura y la intensidad de incidencia de los golpeteos internos.

El proceso de reparación fue detenido a este punto debido a que la simple manipulación (energización y acceso lógico de datos) del dispositivo afectado implicó un progreso acelerado de los primeros síntomas observados en su etapa más temprana de análisis y observación. La exposición prolongada bajo estas condiciones de operación derivaría en la destrucción total del deslizador y, con este, las cabezas de lectura/escritura y superficie magnetizable.

Pese a que el proceso de reparación fue detenido, una posible solución (la cual no será considerada en el presente proyecto de investigación) implicaría la manipulación física de los elementos internos encargados de la lectura y escritura de datos bajo un ambiente controlado, esto, mediante el acoplamiento provisional de elementos idénticos que, de forma funciona, pudieran brindar condiciones estables para la extracción de datos.

A continuación, en la tabla 32, se muestra de forma condensada el conjunto de resultados obtenidos a partir de las pruebas aplicadas al objeto descrito en la figura 51.

ELEMENTO	TIPO DE DAÑO/CARACTERÍSTICAS	MÉTODO UTILIZADO	RESULTADOS
SECTORES DAÑADOS FÍSICAMENTE.	MECÁNICO, CON IMPOSIBILIDAD DEL USUARIO PARA ACCEDER A LOS DISCOS LÓGICOS.	NO APLICA.	SIN RECUPERACIÓN, OPERACIÓN INCONCLUSA.

Tabla 32. Errores, observaciones y resultados obtenidos para un DDE con daños físicos en sectores.

CONCLUSIONES PARCIALES

En esta sección se observó el comportamiento previo a la reparación de un DDE con daños físicos en los sectores de la superficie magnetizable de los platos internos; así mismo, el orden y conjunto de operaciones que definieron su estado de recuperación

Para este DDE, se analiza que el tipo de daño físico impidió de forma permanente el acceso lógico de la información. Al no existir las condiciones y/o medios que permitan este nivel de recuperación, se procede a catalogar a una unidad de DDE como **inaccesible**; con ello se establece que la recuperación fue inconclusa.

2.2.3 CASO REPRESENTATIVO 3: PATRÓN DE RAYADO APLICADO POR EL CABEZAL DIRECTAMENTE AL PLATO MAGNETIZABLE.

Al igual que en los casos de estudio para las fallas lógicas y mecánicas, el en capítulo anterior se estudiaron las propiedades físicas del material compuesto (base de Al con un recubrimiento de Co) del plato magnetizables, así como la jerarquía en la que se mantienen estructurados los datos lógicos (sistema CCS e identificadores DBL).

El plato magnetizable es la figura, en términos reales, más sensible e importante de todo el DDE, esto es, ya que se encuentra a expensas de un motor que le proporcione impulso, movilidad y estabilidad, de un actuador que se mueva por sobre encima de el para interactuar con señales analógicas para ejecutar las funciones de lectura y escritura de datos y, en adición, un sistema computacional (equipo de cómputo fijo y/o portátil) que lo contenga; todos estos elementos adyacentes pueden agregar señales, acciones e influencias que comprometan su funcionamiento y dinámica interna/externa.

Un patrón de rayado en el plato magnetizable **es la condición de carácter permanente e irreversible más desastrosa** que puede acontecer en un DDE pues, atenta en contra la información de forma directa y definitiva. Dicha condición consiste en la destrucción del medio físico donde residen los datos lógicos debido al impacto contundente entre las superficies del deslizador y el disco, se destruye el recubrimiento de Co e incluso la base de Al y/o cristal pulidos.

Se puede establecer que existe un daño por contacto físico cuando suceden una o ambas condiciones siguientes, las cuales, se describen a continuación:

CONTACTO ESTÁTICO

Sucede cuando el DDE se encuentra en estado de reposo, sin energización y con las cabezas dispuestas en su área de estacionamiento (figura 12). Puesto que para este tipo de dispositivos las cabezas “reosan” directamente en una superficie determinada del plato, son susceptibles de sufrir un contacto cuando se le aplica una fuerza externa (caída, golpe lateral y/o incorrecta manipulación de la unidad de DDE). Para estos casos, se produce una fisura localizada y, con ello, no sólo se destruye la superficie del plato magnetizable, sino

que el arreglo de cabezal, deslizador y cabezas implicados (creándose así patrones erráticos de contacto perceptibles e imperceptible).

A continuación, en la figura 51, se observa un daño de este tipo, nótese que el contacto sucedió en la zona más externa del plato, tomando como punto de referencia el eje central del motor. Como caso particular, el cabezal impactó y fisuró en un par de puntos diferentes adyacentes, destruyéndose por completo ambas estructuras implicadas.

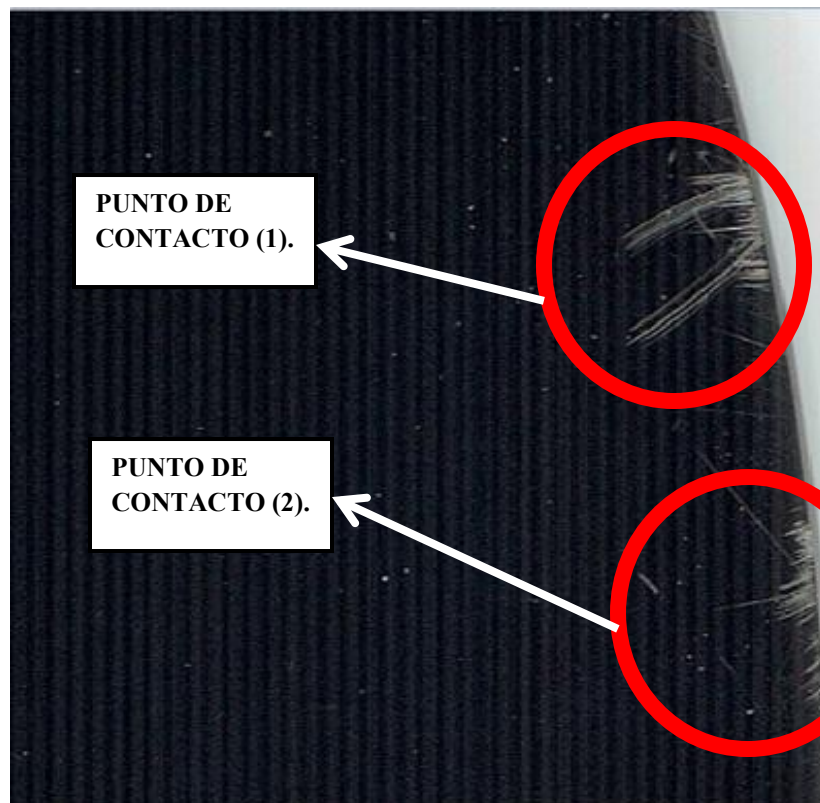


Figura 51. Visualización de una condición de fisura por contacto estático en el borde exterior del disco rígido.

CONTACTO DINÁMICO

Este tipo es el que posee una mayor incidencia; al igual que el anterior, consiste en el contacto físico contundente entre el cabezal y la superficie del plato magnetizable, la destrucción de la información es inminente, sin embargo, este se caracteriza debido a que su extensión de contacto es prolongada y traza un círculo en donde se presenta; en adición, si el DDE contiene múltiples cabezas, el desajuste es tal que puede provocar el contacto con las múltiples caras de los platos. Como es evidente, este sucede cuando el DDE se encuentra funcionando y energizado eléctricamente.

Se puede establecer que este tipo de contacto acontece en cualquiera de las etapas de funcionamiento del dispositivo; las razones por la que sucede son:

1. Si el DDE está acoplado como unidad externa y existe un golpe lateral, las cabezas son impulsadas en contra de los platos cuando la carcasa hace contacto en la superficie de trabajo que sostiene todo el arreglo.
2. Por la caída y/o manipulación incorrecta de un equipo portátil, es decir, la ejecución de movimientos bruscos que no puedan ser asimilados por la carcasa del DDE y se transmiten al actuador.
3. Por aplastamiento, es decir, por la aplicación consistente de una fuerza (peso de algún objeto) directo sobre la cubierta del DDE; el cual, produce un impulso paralelo en las uniones del actuador con la carcasa, dicho impulso provoca una ondulación en el brazo y reacomoda destructivamente el deslizador hacia el plato.

A continuación, en la figura 52, se observa un contacto físico del tipo estudiado, el DDE utilizado está compuesto por un sólo plato magnetizable, nótese que el patrón mostrado en la estructura establece un patrón circular, lo cual, sugiere que el dispositivo sufrió un impacto (caída), el cual sometió a la cabeza en contra del plato y, por el movimiento existente en el mismo, este patrón fue plasmado.

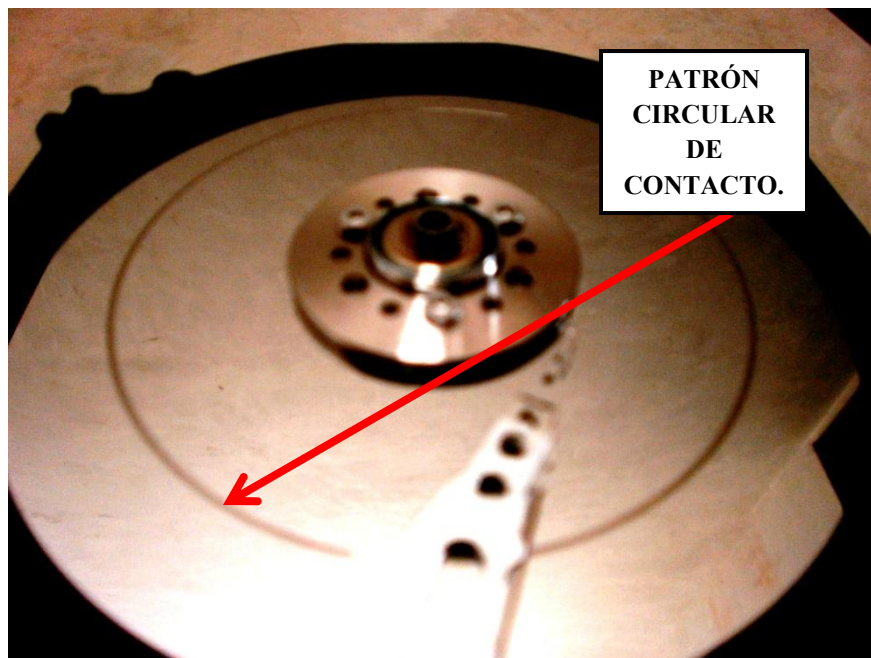


Figura 52. Acercamiento para una condición de rayado físico por contacto dinámico dentro de un DDE.

DESCRIPCIÓN DEL PROCESO DE REPARACIÓN

Considérese, como caso **demostrativo**, en la tabla 33, los datos de placa (y lógicos) de un DDE (figura 53) que presenta un patrón de rayado físico en la estructura de su plato de datos por contacto dinámico.

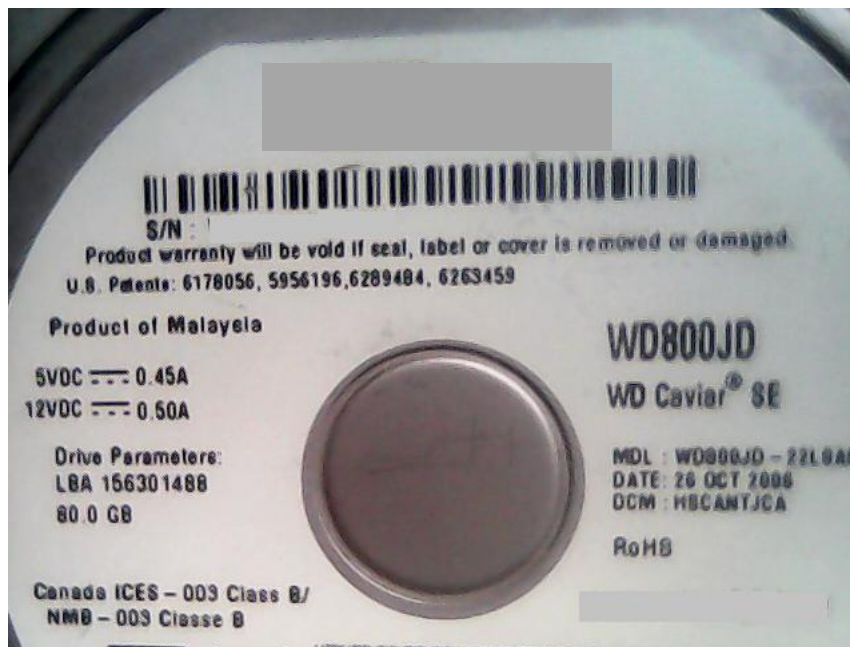


Figura 53. Datos de placa para DDE con daño físico por contacto dinámico del cabezal con el disco rígido.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	WESTERN DIGITAL.
MODELO.	WD800JD.
DBL.	156301488 SECTORES.
INTERFAZ.	SATA.
CAPACIDAD DE ALMACENAMIENTO.	80 GB
VOLÚMENES CONTENIDOS.	DESCONOCIDO.

Tabla 33. Datos de placa (y lógicos) para DDE afectado físicamente en su disco rígido por contacto dinámico.

La falla particular de este DDE tuvo lugar cuando el mismo sufrió una caída de 1.30 metros (cuando se encontraba operando como una unidad externa de almacenamiento),

considerando la altura de su superficie de trabajo hasta el suelo, posterior al impacto, sucedió un rebote y finalmente se detuvo.

Acorde a lo desarrollado en el presente proyecto de investigación, se expondrían el conjunto de técnicas y aplicaciones de *hardware* y *software* tales que permitieran un método de recuperación de datos (parcial y/o total); sin embargo, la condición descrita es considerada como irrecuperable y no admite ningún procedimiento y/o técnica de reparación y, por lo tanto, de extracción de datos.

Como regla universal, todo aquel DDE que posea este tipo de daño físico (perceptible e imperceptible) en sus discos rígidos debe de ser catalogado como **irrecuperable**.

La condición descrita fue determinada en función de la presencia de los siguientes síntomas:

1. El DDE, mediante la utilización de un sistema computacional externo, nunca fue reconocido por el módulo BIOS, por lo tanto, nunca se desencadenaron las instrucciones del módulo *firmware*, sector de inicio y, por consecuencia, su respectivo contenido de la tabla de particiones.
2. Durante su etapa de energización, se observaron fuertes golpeteos del cabezal en contra de la base del motor de eje central y, en adición, sonidos que concuerdan con las cabezas rasgando la superficie del plato.
3. Aun con la alimentación eléctrica disponible, el DDE detuvo su funcionamiento, esto típicamente sucede cuando el cabezal no puede leer el contenido del *software firmware* y, en un intento por no ocasionar daños mayores, detiene el funcionamiento global del dispositivo.
4. Finalmente, la consideración de las características de comportamiento previas y posteriores del equipo a la caída.

A continuación, en la figura 54, se muestra el interior del DDE descrito, nótese la formación de anillos en la superficie del disco rígido, dicha condición es un claro indicador de que, posterior al primer contacto, existieron réplicas que terminaron por destruir otras localidades físicas del plato y del actuador mismo.

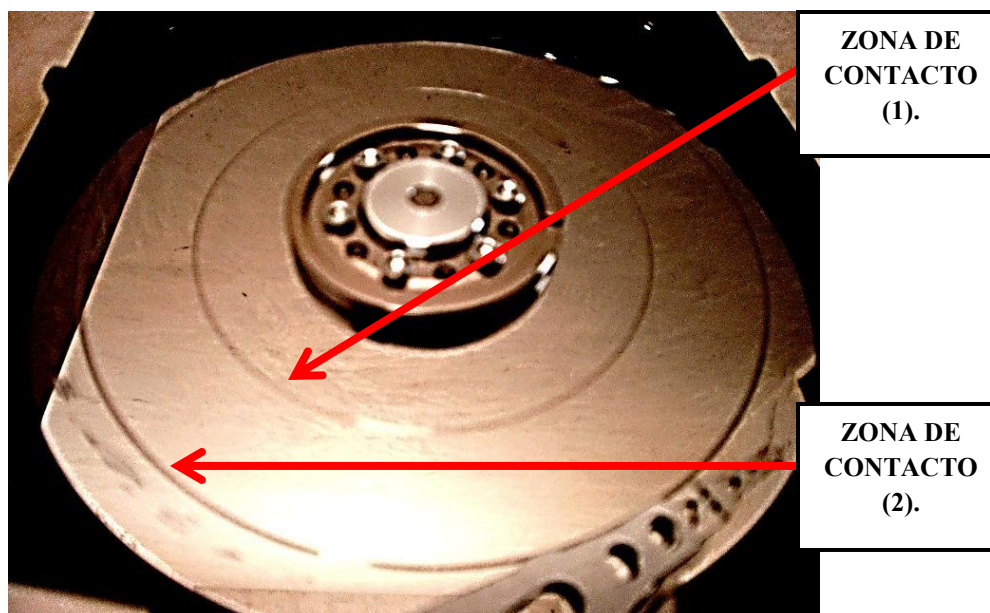


Figura 54. Múltiple patrón de rayado circular en la superficie del disco rígido por contacto dinámico en un DDE.

A continuación, en la tabla 34, se muestra de forma condensada el conjunto de resultados obtenidos a partir de las observaciones y las pruebas aplicadas al objeto descrito en la figura 54.

ELEMENTO	TIPO DE DAÑO/CARACTERÍSTICAS	MÉTODO UTILIZADO	RESULTADOS
PLATOS DAÑADOS FÍSICAMENTE.	MECÁNICO, DESTRUCCIÓN TOTAL DE LA INFORMACIÓN Y EL MEDIO FÍSICO QUE LA CONTIENE.	SIN MÉTODO (NO APLICA).	RECUPERACIÓN NULA/PÉRDIDA TOTAL DE LA INFORMACIÓN.

Tabla 34. Errores, observaciones y resultados obtenidos en un DDE con daños físicos en los platos magnetizables.

CONCLUSIONES PARCIALES

En esta sección se analizaron los efectos, características y observaciones propias para un DDE que ha sufrido un contacto físico y una destrucción de la superficie magnetizable que contiene la información. Ante dicha condición descrita, no existe un método, técnicas y/o implementación posible de *software*, *hardware* y/o *software-hardware* combinados tal que restauren el daño a niveles que permitan la reconstrucción de la información y su respectiva extracción.

Desafortunadamente para el DDE que lo padezca, la condición de contacto físico estático y dinámico, como ya se estudió, es la situación más agresiva (permanente) y severa que un DDE pueda sufrir en contra de sus estructuras mecánicas y lógicas.

En este capítulo se estudiaron las fallas de las estructuras conformantes del DDE, así como los posibles métodos de solución pertinentes. Las estructuras “lógica” y “mecánica” pueden verse afectadas, de forma independiente y/o combinada bajo diferentes circunstancias que les comprometan, ya sea de forma temporal o permanente, y con ellas la información contenida en el DDE. Así mismo, un fallo lógico tiene la capacidad de generar uno mecánico y viceversa; las afectaciones actuantes en las estructuras pueden ser mutuamente incluyentes; y con ello, las maniobras de: detección, reparación, y aplicación de un método de recuperación de datos incrementan considerablemente la complejidad de la actividad expuesta.

Para el presente proyecto de investigación, los métodos de reparación mecánicos implican el generar el conjunto de condiciones físicas tangibles tales que permitan la existencia de la dinámica lógica interna. En tanto que, los métodos de reparación lógicos representan una herramienta de restablecimiento de condiciones virtuales, en las cuales, el principal y primordial objetivo es el de, a partir de la aplicación de *software*, recuperar el conjunto de bytes suficientes capaces de construir cadenas de información útiles y manipulables para y por el usuario.

CAPÍTULO 3. SOFTWARE “FERCUVILL V5.0” PARA LA RECUPERACIÓN DE INFORMACIÓN EN DISCOS DUROS ELECTROMECAÑICOS

Las estructuras: mecánica y lógica conforman la plataforma de operación sobre la cual la información existe y es capaz de ser manipulada mediante técnicas físicas y virtuales por el usuario y/o programas (inclúyase el SO y/o códigos maliciosos). Para el presente trabajo desarrollado, se realizarán procedimientos de recuperación de información mediante un *software* de diseño orientado a la extracción segura de datos a partir de la construcción de un código de programación tal que permita relacionar la lógica de operación de la información con la de funcionamiento del objeto mismo ante condiciones inestables, ya sea por deterioro mecánico y/o de virtual (informático). Para dicho contenido expuesto, el estudio detallado del *software* mencionado será a partir de los siguientes campos:

- **DEFINICIÓN.**
- **CLASIFICACIÓN Y DESCRIPCIÓN DE LOS MÓDULOS.**
- **VISUALIZACIÓN DEL ENTORNO GRÁFICO DE LA INTERFAZ DE OPERACIÓN DEL SOFTWARE “FERCUVILL V5.0”.**
- **CONCLUSIONES PARCIALES.**

Este capítulo debe de ser considerado como el **manual de usuario** del programa, pues, en esta sección se explicarán, expondrán y comprobarán las diferentes herramientas y algoritmos diseñados para recuperar información en unidades de DDE. El *software* “FERCUVILL V5.0” está diseñado para ser efectivo, eficiente y estable en cualquier dispositivo de almacenamiento masivo de datos que tenga un SA y SO compatibles; esto le hace apreciable pues, de necesitarlo, puede ser funcional sobre otros dispositivos de datos tales como: memorias digitales de interfaz tipo USB.

3.1 DEFINICIÓN DE “FERCUVILL V5.0”

El software “FERCUVILL V5.0” se define formalmente como aquel programa de recuperación de información con interfaz gráfica, organizado por módulos y capaz de establecer un conjunto temporal de condiciones virtuales tales que permitan la lectura,

extracción, manipulación y verificación de la información rescatada proveniente de unidades de almacenamiento de datos y, en especial, del DDE.

3.1.1 REQUISITOS PARA LA INSTALACIÓN Y EJECUCIÓN

“FERCUVILL V5.0” es construido y orientado (esencialmente) al tratamiento de unidades de DDE pues, como se ha establecido en el presente proyecto desarrollado de investigación, este dispositivo es aquel que cuenta con la mayor capacidad de almacenamiento físico registrado y, precisamente por dicha propiedad, una condición de fallo (eventos multifactoriales) puede resultar en una pérdida masiva de datos cuyo impacto sea trascendental dentro de un sistema de datos compuesto. Sin embargo, otros dispositivos digitales pueden ser igualmente intervenidos con resultados satisfactorios, básicamente, debido a la compatibilidad de operación. Finalmente, en la tabla 35, se colocan el conjunto de características físicas y virtuales mínimas para soportar la instalación y ejecución en estado permanente del programa citado.

CARACTERÍSTICAS VIRTUALES	CARACTERÍSTICAS FÍSICAS
1) Instalar una versión de SO original, actualizada y registrada base “Windows” [99] a partir del año 2002.	1) Una velocidad de microprocesador igual o superior a 512 MHz (“Mega Hertz”).
2) Contemplar un nivel igual y/o superior a 1024 MB en memoria virtual.	2) Módulo de memoria RAM igual o superior a 512 MB.
3) Contar con una capacidad mínima de memoria RAM igual o superior a 512 MB.	3) Contemplar un espacio libre de almacenamiento de 1 GB en el DDE y/o volumen.
	4) La presencia de puertos USB nativos.

Tabla 35. Recursos físicos y lógicos mínimos de un sistema computacional para la instalación y ejecución del *software* “FERCUVILL V5.0”.

3.2 CLASIFICACIÓN Y DESCRIPCIÓN DE LOS MÓDULOS CONSTITUTIVOS

Los **módulos** se definen como aquellas instancias básicas y complementarias independientes (identificadas en el programa como “*software primario*” y “*software secundario*”) entre sí que ejecutan un grupo de subrutinas (tareas específicas y automáticas) basadas en un algoritmo de programación único, pero que en conjunto, establecen un comportamiento de operación tal en el que el objeto modificado (en este caso, las unidades de almacenamiento de datos) pueda presentar características favorables para implementar una recuperación de información efectiva.

3.2.1 MÓDULOS PRIMARIOS

Se definen como aquellos que conforman al programa medular, pueden ejecutarse independientemente de la presencia de los módulos secundarios. La ausencia de estos se traduce en una inoperancia total del *software* principal. Para el caso particular de “FERCUVILL V5.0”, sus módulos fundamentales están expresados como:

- **MÓDULO 2: S. V. B.**
- **MÓDULO 3: I. C. B.**

Las instancias anteriores se consideran definitivas debido a que son, precisamente, las encargadas de ejecutar los procesos de **recuperación de datos**. A continuación, se procede a describirlos en detalle.

MÓDULO 2: S. V. B.

Se define como aquel programa encargado de, a través de un arreglo de interfaz gráfica y barra de progreso, ejecutar un procedimiento ininterrumpido de extracción de datos de objetos interiores a volúmenes tanto nativos (pertenecientes al SO) como externos (pertenecientes a unidades físicas extraíbles).

CARACTERÍSTICAS DE OPERACIÓN

1. *Software* con altos privilegios de operación.
2. No contempla restricción de copiado de archivos por extensión de caracteres en su ruta lógica y/o por tamaño en disco. Solamente en aquellos con una marcada incapacidad de ser leídos y/o identificados por el SO.
3. Permite la interacción de dispositivos de almacenamiento de datos tanto internos como externos; de la misma forma, si estos son elementos reales (disco físicos) y/o virtuales (disco lógico) a nivel “partición”, o bien, “directorio”.
4. Admite una anulación en su proceso, es decir, que este pueda ser cancelado en algún momento de su operación sin que la información manipulada se vea afectada y/o corrupta por el *software* mismo.
5. El campo “FUENTE” indica la dirección virtual del dispositivo lógico que contiene la información que se desea recuperar.
6. El campo “DESTINO” indica la dirección virtual del dispositivo lógico encargado de almacenar la información cuando esta sea recuperada.
7. A diferencia de otras aplicaciones, la información es duplicada y se mantiene intacta en ambos campos.
8. Contempla una tecnología de identificación de volúmenes, la cual previene un proceso de sobre-escritura de datos. Básicamente indica que la partición identificada como “FUENTE” no podrá ser igual al “DESTINO”.
9. Finalmente, independientemente de la calidad de la información contenida (legibilidad, reconocimiento y/o acceso a esta), el *software* S. V. B. realiza una copia fiel, la cual incluye todas las configuraciones originales del objeto (propiedades).

MÓDULO 3: I. C. B.

Se define como aquel programa encargado de, mediante un arreglo de interfaz por consola semi-automatizada, ejecutar un proceso eficaz de extracción de datos a partir de la implementación de una ventana emergente con algoritmo de programación específico.

A diferencia del módulo anterior, este permite la recuperación de la información en dispositivos cuyas propiedades (mayoritariamente físicas y minoritariamente lógicas) eviten la correcta manipulación de los datos (edición) a través de métodos convencionales.

CARACTERÍSTICAS DE OPERACIÓN

1. *Software* con altos privilegios de operación.
2. No contempla restricción de copiado de archivos por extensión de caracteres en su ruta lógica y/o por tamaño en disco.
3. Para los archivos con problemas de lectura identificados, intenta obtener la mayor cantidad de información del objeto, conservando la integridad del mismo sin estresar físicamente el sector (sectores), pistas y cilindros que la contengan.
4. Permite la interacción de dispositivos de almacenamiento de datos tanto internos como externos; de la misma forma, si estos son elementos reales (disco físicos) y/o virtuales (disco lógico).
5. A diferencia del módulo anterior, este no admite la anulación del proceso de forma controlada. Esto es, una vez iniciado el procedimiento este debe de permanecer estrictamente intacto, de lo contrario, la información copiada puede sufrir una corrupción (la información de la ruta original se mantiene intacta).
6. El campo “**DISCO_1**” indica la dirección virtual del dispositivo lógico que contiene la información que se desea recuperar.
7. El campo “**DISCO_2**” indica la dirección virtual del dispositivo lógico encargado de almacenar la información cuando esta sea recuperada.
8. De la misma forma que el *software* S. V. B., la información se mantiene intacta en ambas direcciones lógicas, sin embargo, el módulo I. C. B. permite obtener la copia de volúmenes completos en lugar de directorios individuales.
9. La información solicitada en los campos “**DISCO_1** y **DISCO_2**” debe de proporcionarse tal cual se solicita en la ventana emergente, es decir, colocar el par de puntos verticales inmediatamente después de la letra de la unidad establecida.
10. Una tecnología para evitar la sobre-escritura se encuentra asida a este *software*, de seleccionarse la misma unidad para el proceso de copiado, la ventana emergente

indicará el error y el proceso de selección de disco lógicos deberá de ser especificado nuevamente.

3.2.2 MÓDULOS SECUNDARIOS

Estos se definen a su vez como aquel conjunto de programas complementarios a los módulos primarios, su ejecución depende exclusivamente de que un objeto con mayor jerarquía los invoque. Sin embargo, su presencia permite que el *software* modular opere de una forma estable y, como consecuencia directa, la información recuperada posea una estructura lógica aceptable para ser editada. Para el caso particular del programa “FERCUVILL V5.0”, sus módulos secundarios son:

- **MÓDULO 0: J. J. B. V.**
- **MÓDULO 1: I. C. V.**
- **MÓDULO 4: V. H. B. V.**
- **MÓDULO 5: P. A. H.**
- **MÓDULO 6: S. H. B. V.**
- **MÓDULO 7: H. A. A. B.**

Las instancias anteriores permiten, en su conjunto: controlar, editar, limpiar, organizar, presentar, reparar, establecer y mantener todo aquel conjunto de datos contenidos en una unidad de almacenamiento de datos. La ausencia y/o funcionamiento parcial de estos derivaría directamente en la producción de copias corruptas de información cuyos daños, eventualmente, terminarían por degradar el respaldo obtenido hasta el punto de la destrucción lógica.

MÓDULO 0: J. J. B. V.

Este complemento de control es el primero presente en el programa; se define como aquel encargado, mediante la utilización de un par de campos de texto, de proporcionar acceso a la aplicación de carga de elementos.

CARACTERÍSTICAS DE OPERACIÓN

1. Mediante una doble solicitud de datos, le indica al usuario que ingrese la información requerida para desencadenar la descarga en memoria de los demás módulos adyacentes.
2. Esta tecnología se implementó como una medida de seguridad ante el uso indebido y/o no permitido de “FERCUVILL V5.0”.
3. Este módulo está diseñado con un algoritmo de cifrado de datos en combinación con una cadena de caracteres múltiples, de los cuales, se destacan, dígitos numéricos y símbolos en código ASCII [6].

MÓDULO 1: I. C. V.

Este complemento, en conjunto con el anterior expuesto, constituye todo el marco de protección del programa expuesto. El presente módulo está diseñado para evitar la usurpación del control de “FERCUVILL V5.0”, ya que, existen *softwares* maliciosos encargados de “manipular” otros programas para que, bajo determinadas circunstancias, estos operen de forma errónea y/o “contribuyan” en el proceso infeccioso hacia otras partes del SO y/o hacia otros equipos computacionales externos.

CARACTERÍSTICAS DE OPERACIÓN

1. En una primera etapa, le solicita al usuario que ejecute la descarga en memoria de los *softwares*/módulos primarios y secundarios, posteriormente, se ejecutará el programa medular.
2. El usuario recibirá un mensaje de estado en el que se le indica si la carga de los elementos (mencionados anteriormente) fue exitosa y/o si existieron errores.
3. Posteriormente, en una segunda etapa, el usuario tendrá que interactuar directamente con el programa, pues, se le solicitará que (mediante el uso del teclado del sistema computacional) escriba la “palabra de control”. Esta tecnología se utiliza típicamente para comprobar que, en efecto, un humano está manipulando el programa y no así otro *software* del tipo “virus informático”.

4. Una vez que el usuario sea capaz de escribir el texto indicado, de forma automática, se habilitará la opción para mostrar en pantalla la ventana de control del *software* medular.

MÓDULO 4: V. H. B. V.

Este programa es el encargado de ejecutar la administración sobre el proceso de completado de todos los demás módulos secundarios, esto es; existen ciertas tecnologías de recuperación de datos que requieren de un reinicio y/o apagado total del SO; es en ese momento cuando el módulo mencionado es capaz de proporcionar dicha característica y, de esa forma, aplicar las modificaciones realizadas a la información.

CARACTERÍSTICAS DE OPERACIÓN.

1. Provee de un servicio avanzado de “arranque” y/o reinicio diferente del convencional, este está especialmente diseñado para atender las modificaciones lógicas realizadas por los módulos primarios y secundarios inmediatos a este.
2. Es un *software* de control, pues, permite invocar la habilitación y/o inhabilitación de ciertos módulos dependientes. La razón de implementar esta tecnología radica en que, en la totalidad de los escenarios de recuperación de datos, ciertas dependencias lógicas del SO necesarias para ejecutar a “FERCUVILL V5.0” se encuentran parcial y/o totalmente desactivadas/dañadas. Entonces, esta característica permite generar (de forma temporal) esas dependencias a fin de ser usadas para la ejecución del programa mismo.
3. Este módulo ha sido programado para invocar un par de potentes herramientas virtuales conocidas como: MÓDULO A: K.L.G. y MÓDULO B: A.J.L.; la primera de estas permite mostrar un diagnóstico general sobre el estado de operación y funcionamiento físico del DDE donde reside “FERCUVILL V5.0”, en tanto que el segundo crea una localidad segura y aislada de infecciones y acceso no autorizado solamente accesible por el usuario original y propietario de la información.

MÓDULO 5: P. A. H.

Este complemento secundario contiene una característica de propiedad, es decir, otorga la capacidad al usuario de tomar posesión de objetos (carpetas y archivos contenidos en estas) que han sido alterados en dicha estructura. Típicamente, un objeto pertenece, primeramente el SO y en segundo plano al usuario asociado a este, sin embargo y ante un ataque por código malicioso, el usuario puede perder la pertenencia de dicho objeto y no ser capaz de modificarlo, eso incluye sus procesos de copiado y extracción.

CARACTERÍSTICAS DE COMPORTAMIENTO

1. Mediante la ejecución del módulo, el usuario no observará algún cambio aparente, sin embargo, este podrá localizar un nuevo campo identificado como “FORZAR PROPIEDAD” en el menú contextual del objeto de interés a ser recuperado.
2. Es necesario seleccionar dicho campo para poder adquirir nuevamente el control sobre el objeto, de esa forma, cualquier otro elemento (interno y/o externo al SO) ajeno no tendrá acceso y la información podrá ser editada libremente.
3. Contiene un segundo módulo de desactivación, el cual, revierte la característica descrita en el punto número 1. Dicha inhabilitación es necesaria cuando, previo a realizar un escaneo mediante un *software* antivirus, el objeto deba de ser controlado por otro programa del SO mismo, entonces se deberá de ceder dicho control.
4. Los procedimientos de este módulo no interfieren con el comportamiento del equipo, pero solamente debe de aplicarse a objetos que genuinamente pertenezcan al usuario y no así al SO, de lo contrario, se estará atentando contra este y la información contenida estaría en riesgo de bloqueo.
5. Para habilitar y/o deshabilitar la característica, es necesario seleccionar la opción deseada y aplicar un reinicio del SO de forma inmediata.
6. **Este programa provee de una interfaz de anulación de procesos parásitos, es decir, detecta a otro tipo de programas que interfieran de forma directa con otro “principal”, elimina dicha relación y permite al programa/objeto original trabajar de forma ininterrumpida.**

MÓDULO 6: S. H. B. V.

Este módulo conforma una de las características más apreciables del *software* medular mismo. Virtualmente, permite implementar una protección en tiempo real para anular el proceso infeccioso de amenazas residentes de un SO actuantes en dispositivos de interfaz de conexión USB (arreglos de DDE externo y/o memorias digitales). Si bien la amenaza aún existe de forma local, esta no podrá afectar otros dispositivos no nativos.

CARACTERÍSTICAS DE OPERACIÓN

1. Tecnología autónoma de operación permanente en puertos USB para la anulación del proceso contagioso de dispositivos compatibles con dicha interfaz.
2. Contiene un par de opciones de configuración: para iniciar y detener la aplicación.
3. Posterior a la selección del comportamiento deseado, es necesario aplicar inmediatamente un reinicio del SO.
4. El usuario tiene completo control del comportamiento de la tecnología, esta se ha programado para que (posterior a cada cambio) se realice una limpieza interna de las dependencias implicadas, de esa forma se garantiza la eliminación de remanentes que intervengan de forma nociva.
5. Este procedimiento no afecta la posibilidad del usuario para utilizar el dispositivo de almacenamiento, es decir, la información allí contenida puede ser editada y manipulada.

MÓDULO 7: H. A. A. B.

Este es un *software* avanzado de funcionamiento por ventana emergente capaz de restablecer las propiedades originales de un archivo hasta el punto exacto en el que fueron modificadas, es decir, tales como: capacidad de lectura y escritura; recuperando así el contenido de los objetos.

CARACTERÍSTICAS DE OPERACIÓN

1. El usuario debe de especificar el volumen, partición y/o disco lógico que desee recuperar, esta herramienta aplicará un desbloqueo y un restablecimiento de todos los elementos allí contenidos.

2. Por seguridad, se excluyen de este procedimiento a aquellos archivos nativos del SO necesarios para el correcto funcionamiento de la unidad, sin embargo, los restantes (incluida la información del usuario) objetos son incluidos y modificados de forma efectiva.
3. Dependiendo de la longitud del volumen, el tipo de archivos y la extensión (tamaño) de los mismos, es que se establecerá un rango de tiempo mayor o menor para intervenir todo el disco lógico.
4. Cuando el programa termine su funcionamiento, el usuario recibirá un mensaje en pantalla y podrá cerrar dicha ventana emergente.
5. Llegado a este punto, es necesario aplicar un reinicio del SO, la razón principal radica en que este último considera las modificaciones como “temporales” hasta que no se aplique una detención e inicio del explorador de archivos, por lo tanto, es necesario para aplicar las nuevas configuraciones.

La combinación estable de los módulos primarios y secundarios tendrá como consecuencia directa que el *software* medular opere de forma continua sin inconvenientes.

A su vez, el ***software medular*** se define como aquel arreglo de programación central de administración, control y organización de elementos interdependientes orientados a la ejecución de procesos lógicos dentro de un SO residente.

El programa de diseño “FERCUVILL V5.0” está facultado para funcionar como un programa residente del sistema computacional, pero igualmente puede operar como uno externo, por lo tanto, no dependerá de la actual integridad del SA, SO y/o códigos externos no identificados que pudiesen alterar su comportamiento y el de la unidad de DDE analizada.

Para los casos de estudio expuestos en el capítulo siguiente, el programa se encontrará ejecutándose como externo y con altos privilegios de operación; cada DDE estará conectado a partir de su interfaz nativa.

3.3 VISUALIZACIÓN DEL ENTORNO GRÁFICO DE LA INTERFAZ DE OPERACIÓN DEL *SOFTWARE* “FERCUVILL V5.0”.

El apartado siguiente muestra las capturas en pantalla del programa presentado correspondientes a cada uno de los módulos descritos previamente, así mismo, se enfatizarán sus funciones y/o comportamiento de operación. Posterior a la captura correspondiente, se colocarán en tablas las descripciones necesarias. Dichos procedimientos de reparación y restablecimiento de información pueden ser aplicados para efectuar las modificaciones apropiadas bajo condiciones específicas y, en consecuencia, producir un estado tal en el que el procedimiento total sea considerado como viable.

3.3.1 VENTANA DE INICIO

“FERCUVILL V5.0” permite ser invocado a través de un archivo ejecutable de extensión “.exe”; una vez que se encuentra operando en primer plano, mostrará al usuario la consola de presentación del mismo, es decir, una ventana de control que permite la ejecución y/o cierre de la aplicación sin la necesidad de, primeramente, acceder a otras instancias del *software* modular (figura 55).



Figura 55. Ventana de inicio principal del programa “FERCUVILL V5.0”.

Los elementos de la figura 55 son descritos a continuación en la tabla 36.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	NOMBRE Y DATOS DEL PROGRAMA.
2	BOTÓN DE DESCARGA DE ELEMENTOS.
3	BOTÓN PARA CERRAR DE FORMA GLOBAL EL <i>SOFTWARE</i> .
4	MUESTRA INFORMACIÓN ADICIONAL SOBRE LA VERSIÓN DEL <i>SOFTWARE</i> .

Tabla 36. Descripción de los elementos estructurales de la ventana de inicio del *software* “FERCUVILL V5.0”.

3.3.2 MÓDULO 0: J. J. B. V.

Posterior a la ventana de inicio (y presionando el botón “INICIAR”) se visualiza la primera de dos ventanas de autenticación para la utilización del programa. En esta, el usuario tiene que insertar la información correcta para poder continuar con la ejecución de forma regular.

Por cuestiones evidentes de seguridad e integridad del programa, los datos de inicio solamente están controlados por el creador del *software* mismo (figura 56).

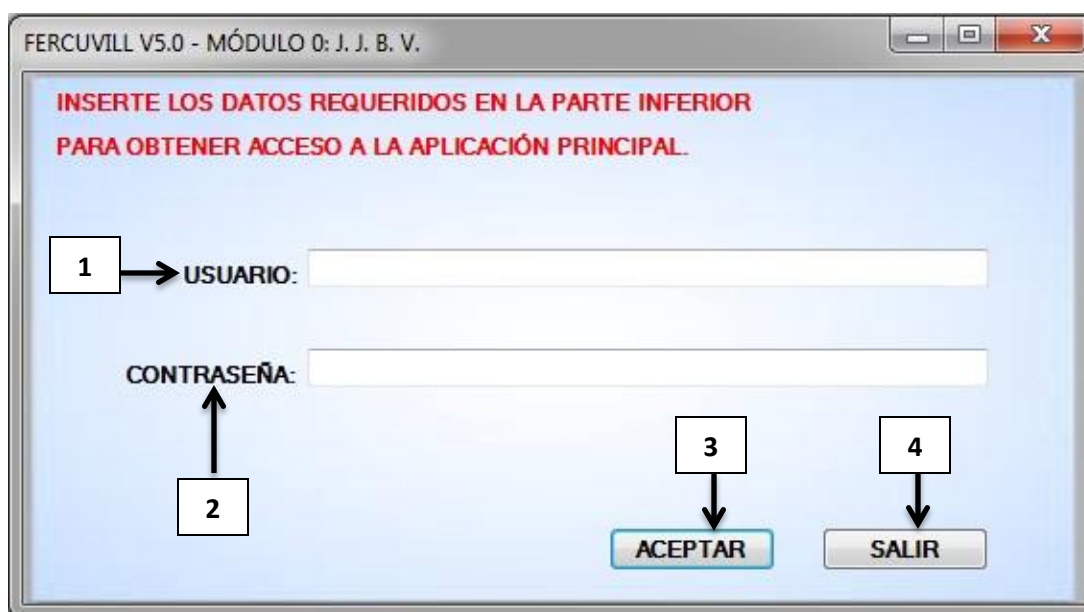


Figura 56. Ventana de control de acceso por autenticación de identidad, MÓDULO 0: J.J.B.V del *software* “FERCUVILL V5.0”.

Los elementos de la figura 56 son descritos a continuación en la tabla 37.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	PALABRA DE CONTROL (1).
2	PALABRA DE CONTROL (2).
3	BOTÓN PARA E INICIAR EL <i>SOFTWARE</i> MEDULAR.
4	DETENER DE FORMA GLOBAL LA EJECUCIÓN DEL <i>SOFTWARE</i> .

Tabla 37. Descripción de los elementos estructurales del MÓDULO 0: J.J.B.V del *software* “FERCUVILL V5.0”.

Este módulo contempla la siguiente configuración:

- Si alguno de los caracteres, independientemente del campo del que se trate, está incorrecto, la aplicación se emitirá un mensaje en pantalla como se muestra a continuación (figura 57):

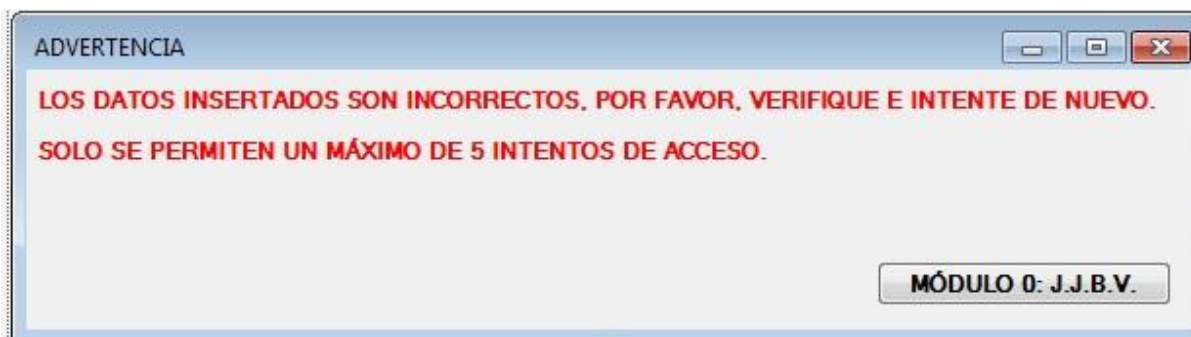


Figura 57. Mensaje del sistema (1): mostrado por la incorrecta especificación de los campos de acceso.

- Una vez que se han excedido el número máximo de intentos; el módulo al mando cerrará abruptamente el programa, de tal forma que, el usuario deberá de ejecutarlo nuevamente.

3.3.3 MÓDULO 1: I. C. V.

Esta segunda ventana de autenticación está diseñada para proteger a “FERCUVILL V5.0” de ser usurpado y/o controlado por *software* malicioso automatizado, es decir, aquel cuyo algoritmo de programación externo falsifica la identidad de un usuario para tomar control de otra aplicación. Los módulos que conforman al *software* propuesto son sensibles y deben de protegerse ante este tipo de daños, de allí la necesidad de implementar la tecnología descrita.

Este módulo contempla la siguiente configuración:

Carga de elementos:

Esta etapa permite la habilitación de los módulos primarios de copiado, de los secundarios para utilidades de propiedades de los objetos y, finalmente, la consola gráfica de control y administración de los mismos.

Sin una etapa de inicio de módulos, el *software* es incapaz de invocar una tarea y/o efectuar una técnica virtual de recuperación de datos.

Comprobación de control:

En esta etapa se le indica al usuario que debe de insertar una determinada palabra en un espacio asignado; una vez completada esa tarea, un botón otorgará acceso total a “FERCUVILL V5.0”, el cual, estará disponible para ser ejecutado.

Los *softwares*: J.J.V.B e I.C.V. constituyen las líneas de protección, seguridad y habilitación de todas las herramientas disponibles. Dichos módulos cuentan con una protección ante “ataques por directorio”, lo cual significa que algún código malicioso envíe masivamente todas las posibles combinaciones de dígitos (signos, letras, números y caracteres) que permitan conceder acceso.

A continuación, en la figura 58, se muestra el ambiente gráfico del MÓDULO 1: I.C.V.; la ventana de ayuda e instrucciones y las barras de progreso para indicar el avance particular y global de los objetos implicados. Al final de la carga de los mismos, el usuario recibirá un mensaje de confirmación y/o de error; de ser así se deberá de ejecutarlo nuevamente.

FERCUVILL V5.0 -MÓDULO 1: I. C. V.

BIENVENIDO AL ASISTENTE DEL SOFTWARE "FERCUVILL V5.0". ESTE LE GUIARÁ EN LOS PASOS NECESARIOS PARA EJECUTAR LA APLICACIÓN DE FORMA CORRECTA.

SIGA LAS INSTRUCCIONES MARCADAS CON LAS INSIGNIAS (1) , (2) Y (3) LOCALIZADAS EN LA PARTE INFERIOR DE ESTA VENTANA, SIRVASE DE LA VENTANA DE AYUDA LOCALIZADA EN LA ESQUINA INFERIOR DERECHA.

ADVERTENCIA:

"NO EJECUTAR LA SECUENCIA INDICADA EN EL ORDEN CORRECTO PRODUCIRÁ QUE EL SOFTWARE OPERE DE FORMA ERRÁTICA".

ELEMENTOS:

- CARGANDO LA INTERFAZ DE USUARIO, ESPERE UN MOMENTO.
- CARGANDO SOFTWARES PRIMARIOS, ESPERE UN MOMENTO.
- CARGANDO SOFTWARES SECUNDARIOS, ESPERE UN MOMENTO.
- CARGANDO SOFTWARE MEDULAR, ESPERE UN MOMENTO.

PROGRESO GENERAL:

1

3

(2) ESCRIBA LA PALABRA "ACTIVAR" EN EL CUADRO DE TEXTO INFERIOR.

(1) INICIAR LA CARGA DE ELEMENTOS

(3) INICIAR EL SOFTWARE

SALIR

4

2

5

VENTANA DE AYUDA

- 1) LOCALIZAR EL BOTÓN UBICADO EN LA ESQUINA INFERIOR IZQUIERDA LLAMADO "INICIAR LA CARGA DE LOS ELEMENTOS"
- 2) UNA VEZ LOCALIZADO, PRESIONARLO Y ESPERAR A QUE LA ACCIÓN SE COMPLETE, USTED RECIBIRÁ UN MENSAJE DE CONFIRMACIÓN.
- 3) POSTERIORMENTE, EN LA ZONA CENTRAL INFERIOR SE UBICA UN MENSAJE QUE SOLICITA ESCRIBIR LA PALABRA "ACTIVAR" DENTRO DE UN CUADRO DE TEXTO, PROCEDA A REALIZARLO Y OBSERVE QUE EL BOTÓN LLAMADO "INICIAR EL SOFTWARE" SE HA ACTIVADO.
- 4) FINALMENTE, PRESIONE ESTE ÚLTIMO BOTÓN Y SE LE CONCEDERÁ ACCESO AL SOFTWARE EN SU VERSIÓN PROFESIONAL.

Figura 58. Ventana de control para carga de elementos y acceso por verificación de texto, MÓDULO 1: I.C.V.

Los elementos de la figura 58 son descritos a continuación en la tabla 38.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	BOTÓN DE DESCARGA PARA ARRANQUE DE <i>SOFTWARES</i> PRIMARIOS Y SECUNDARIOS.
2	ESPACIO ASIGNADO PARA COLOCAR LA PALABRA DE CONTROL.
3	BOTÓN DE HABILITACIÓN DE LA ENTRADA PRINCIPAL PARA EL <i>SOFTWARE</i> MEDULAR.
4	BARRAS DE PROGRESO PARA INDICAR LOS AVANCES INDIVIDUALES Y GLOBALES.
5	DETENER DE FORMA GLOBAL LA EJECUCIÓN DEL <i>SOFTWARE</i> .

Tabla 38. Descripción de los elementos estructurales del MÓDULO 1: I.C.V. del *software* “FERCUVILL V5.0”.

Particularmente para el objeto 1 de la figura 58, cuando la carga de los elementos esté plena y correctamente completada, el usuario recibirá un mensaje en pantalla tal y como se muestra a continuación (figura 59):

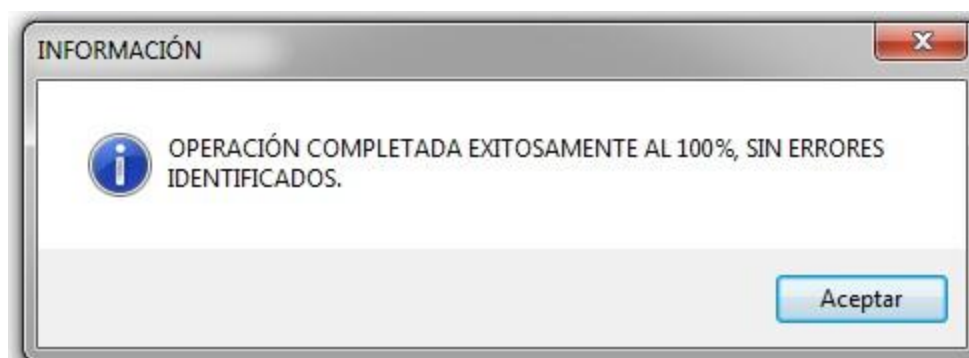


Figura 59. Mensaje del sistema (2): para una carga exitosa de los elementos.

Así mismo, cuando exista algún error en dicho procedimiento, el usuario recibirá a cambio otro tipo de mensaje (figura 60).

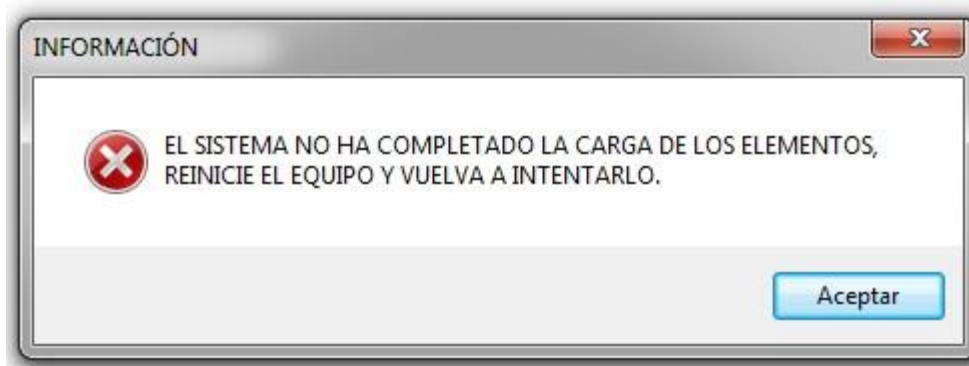


Figura 60. Mensaje del sistema (3): para una carga incorrecta de los elementos .

El *software* “FERCUVILL V5.0” mostrará este último mensaje en pantalla cuando se cumplan una o más de las siguientes condiciones:

1. Cuando los requerimientos expresados en la tabla 35 se cumplan solamente para instalación y no así para la ejecución del programa. Tanto para los lógicos como físicos.
2. Cuando alguno de los módulos no se encuentre disponible y/o bloqueado por algún *software* externo.
3. Cuando, posterior a la instalación del programa, no se efectúe un reinicio del SO.

Finalmente para este módulo, de forma complementaria, se muestra una venta de información adicional (figura 61) para que el usuario, si en determinada instancia lo necesita, pueda auxiliarse y continuar en la ejecución del programa expuesto.

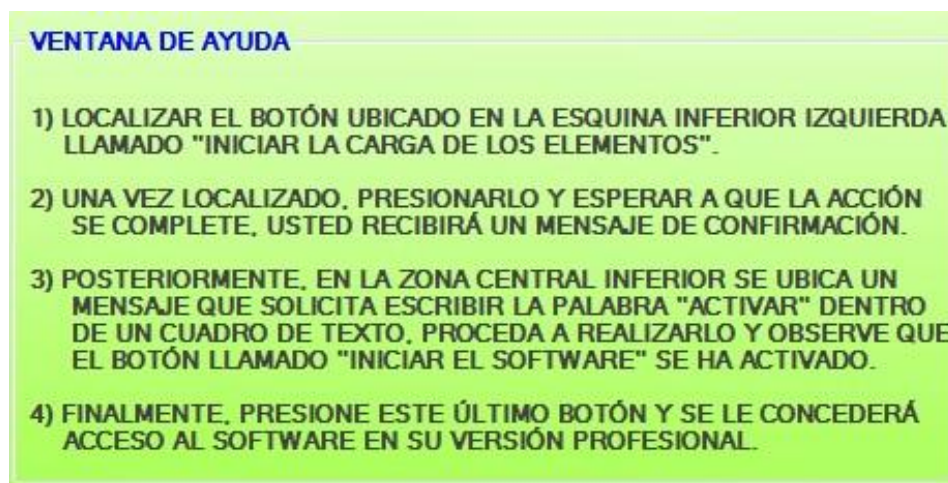


Figura 61. “VENTANA DE AYUDA” del MÓDULO 1: I.C.V. para acceso a la aplicación principal.

Una vez que el usuario siga las instrucciones especificadas en el módulo anterior, se le mostrará la interfaz de control gráfica del *software* medular (figura 62), desde allí podrá invocar todos los módulos primarios y secundarios estudiados orientados a la recuperación y tratamiento de la información.

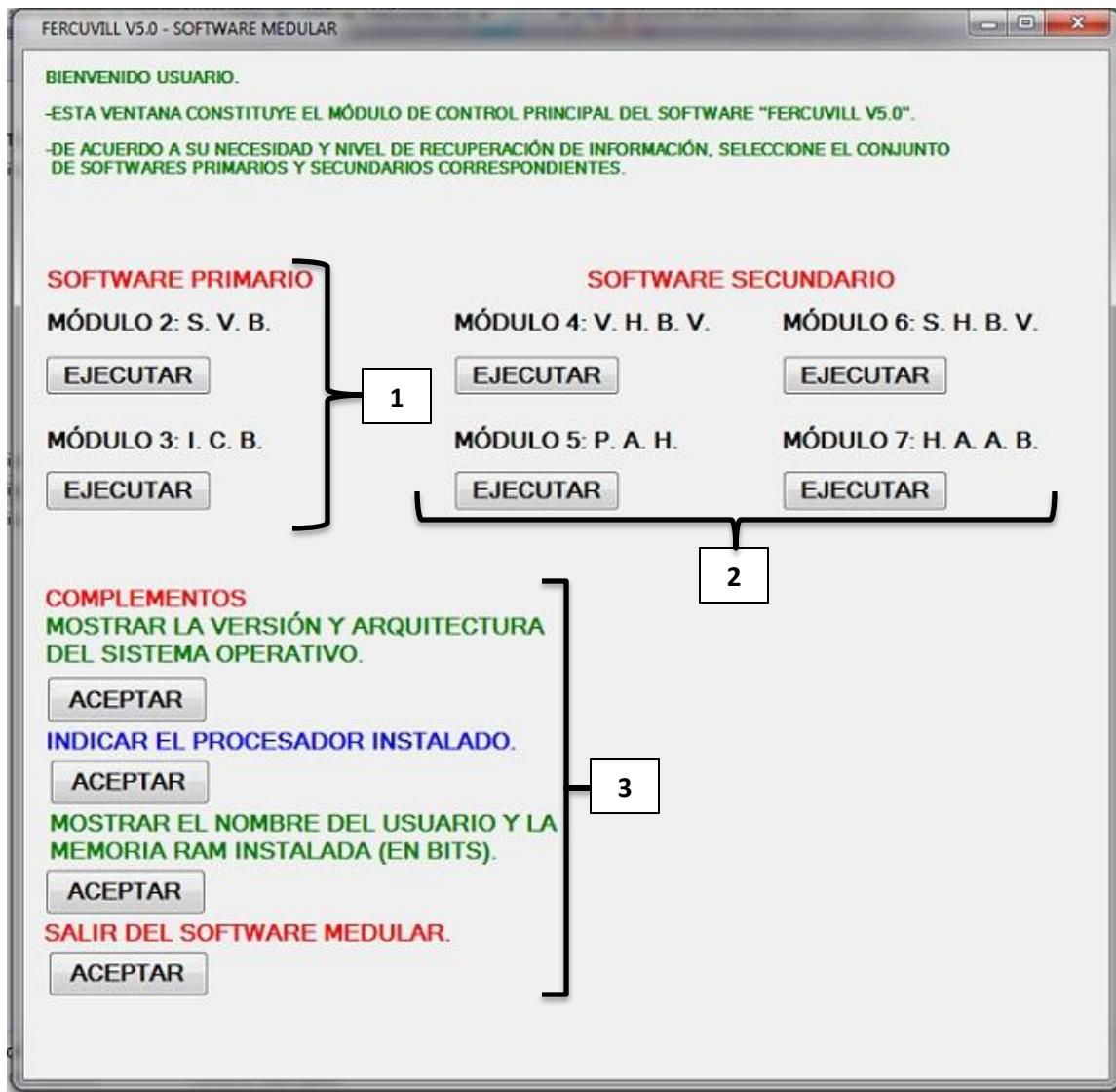


Figura 62. Ventana principal de operación del *SOFTWARE* MEDULAR.

La sección “COMPLEMENTOS” está diseñada para ayudar al usuario a identificar los componentes físicos y lógicos del equipo computacional sobre el cual se está ejecutando el *software* medular.

Los elementos de la figura 62 son descritos a continuación en la tabla 39.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	INDICA LOS DIFERENTES TIPOS DE PROGRAMAS PARA EL COPIADO DE INFORMACIÓN.
2	INDICA LOS DIFERENTES TIPOS DE PROGRAMAS DISPONIBLES PARA EL TRATAMIENTO DE LAS PROPIEDADES DE LA INFORMACIÓN.
3	EN SU CONJUNTO, MUESTRAN INFORMACIÓN DE <i>HARDWARE</i> Y <i>SOFTWARE</i> DEL EQUIPO COMPUTACIONAL ASOCIADO A “FERCUVILL V5.0”.

Tabla 39. Descripción de los elementos estructurales del *SOFTWARE* MEDULAR.

La exposición de los módulos siguientes será a partir de dicha ventana principal; siendo así, el arreglo de programas que sigue en su estudio es aquel relacionado a los *softwares* primarios.

3.3.4 MÓDULO 2: S. V. B.

Este programa (figura 63) cuenta con instrucciones consecutivas para que el usuario pueda recuperar su información de volúmenes identificados por el SO, pero que por influencias de otro tipo de programas, este ha perdido sus propiedades de lectura, escritura e incluso su fecha de creación/modificación. Este módulo presenta las siguientes ventajas de uso:

1. Control gráfico para la identificación de las rutas de “origen/fuente” y “destino” de la información.
2. Visualización de una barra de progreso en la que se indican: las rutas utilizadas, el objeto actual copiado, y la velocidad de escritura aproximada para que la operación sea concluida.
3. Permite cancelar la operación en cualquier momento que el usuario lo decida.

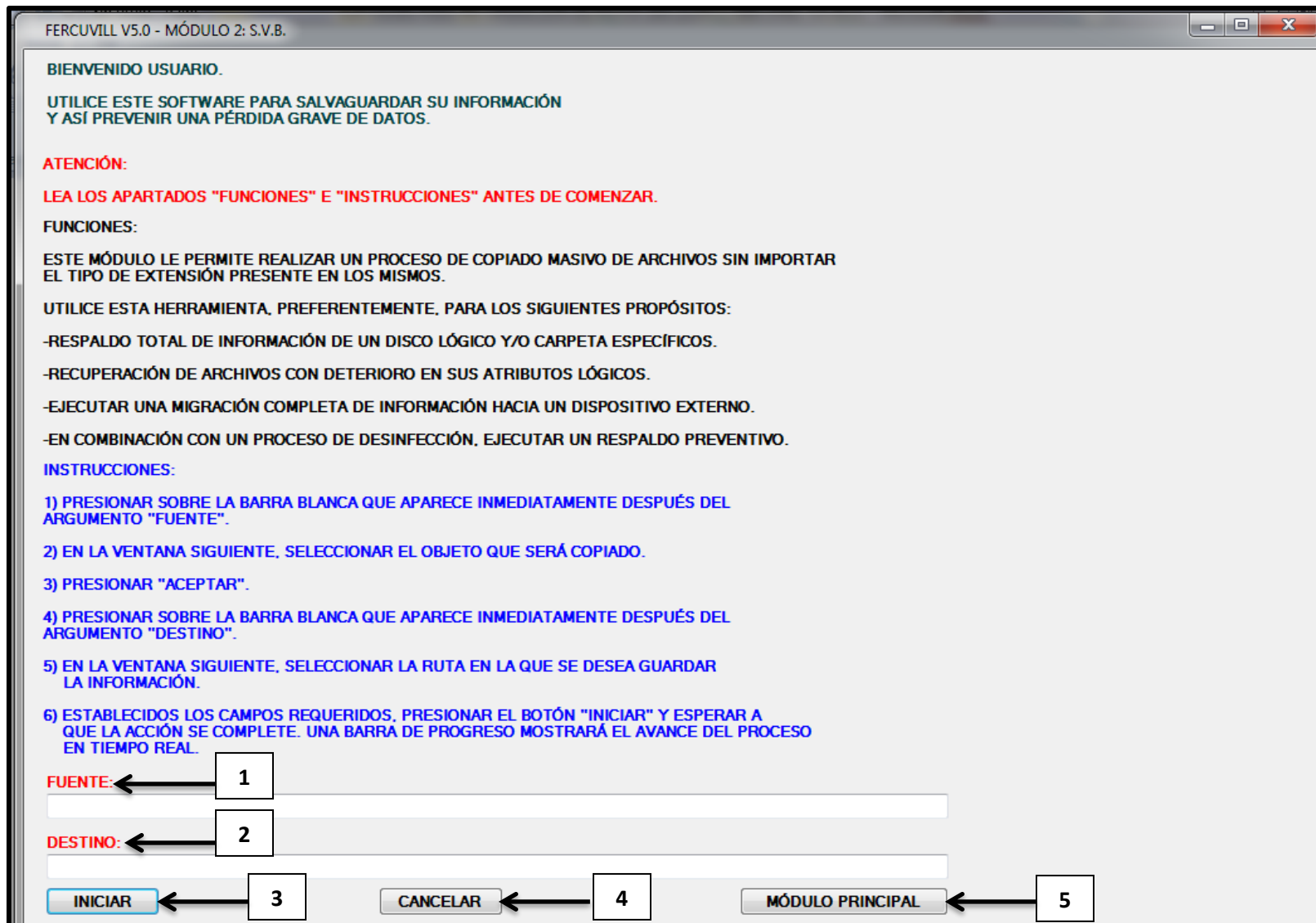


Figura 63. Ventana principal de operación del *software* primario S.V.B.; visualización de "FUNCIONES" e "INSTRUCCIONES".

Los elementos de la figura 63 son descritos a continuación en la tabla 40.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	INDICA LA PARTICIÓN, CARPETA Y/O LOCALIDAD ESPECÍFICA EN LA CUAL RESIDE LA INFORMACIÓN.
2	INDICA EL ESPACIO FÍSICO Y LÓGICO ASIGNADO PARA CONTENER LA INFORMACIÓN RECUPERADA.
3	DESENCADENA LA SECUENCIA DE COMANDOS PARA INICIAR EL PROCESO DE EXTRACCIÓN DE DATOS, MUESTRA UNA BARRA DE PROGRESO.
4	CIERRA EL MÓDULO 2: S.V.B. SIN EFECTUAR CAMBIOS.
5	MUESTRA EN PANTALLA EL <i>SOFTWARE</i> MEDULAR.

Tabla 40. Descripción de los elementos estructurales del MÓDULO 2: S.V.B. del *software* “FERCUVILL V5.0”.

Para este módulo, al igual que el siguiente, se ha instalado una tecnología para evitar la corrupción de datos por sobre-escritura, para el caso en el que se seleccione la misma ruta para los campos “FUENTE” y “DESTINO”, el *software* mostrará en pantalla (figura 64) la siguiente captura:

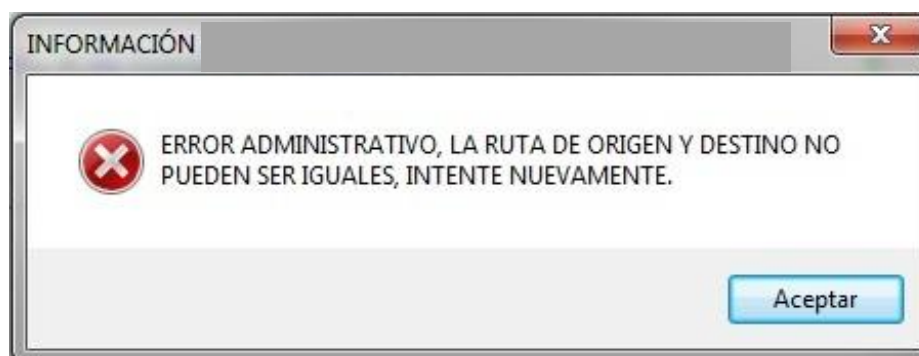


Figura 64. Mensaje del sistema (4): para iteración entre las unidades de “FUENTE” y “DESTINO”.

A continuación, para los puntos 1, 2, y 3, respectivamente, se muestran las capturas en pantalla para cada una de las configuraciones. Nótese que, en complemento con el *software* expuesto, el usuario puede crear una carpeta durante la fase de extracción, si y sólo si esta no ha sido establecida previamente en el DDE y/o disco lógico receptor (figura 65).



Figura 65. Ventana secundaria para la selección de ruta “FUENTE” del volumen seleccionado.

Una vez establecido el origen de la información, el usuario debe de especificar la ruta de destino (figura 66) correcta, puede ser incluso un volumen completo (la información almacenada previamente en el disco lógico “DESTINO” no se verá afectada).



Figura 66. Ventana secundaria para la selección de ruta de “DESTINO” del volumen dispuesto.

Como un ejemplo práctico, una selección correcta de una carpeta que se desea copiar hacia otra localidad contenida en un volumen completo estaría definida como sigue a continuación (figura 67).



The image shows a graphical user interface for configuring a backup. It has two text input fields. The first field is labeled 'FUENTE:' and contains the path 'C:\Users\Computadora\Desktop\INFORMACIÓN A RESPALDAR'. The second field is labeled 'DESTINO:' and contains 'G:\UNIDAD DE RESPALDOS'. Below the fields are three buttons: 'INICIAR' (highlighted in blue), 'CANCELAR', and 'MÓDULO PRINCIPAL'.

Figura 67. Ejemplo para la selección de una “FUENTE” y “DESTINO” en el MÓDULO 2: S.V.B. para un respaldo de información entre un volumen y un DDE externo.

Una vez el usuario decida proceder, se ejecutarán las líneas de comando y la información existirá en ambas localidades, completando así un proceso seguro de extracción de datos y, rescatando de igual forma, las propiedades de cada uno de los objetos contenidos en el volumen.

3.3.5 MÓDULO 3: I. C. B.

Este módulo se encuentra dispuesto en un par de etapas: una gráfica (figura 68) y otra por consola de operación externa semi-automatizada (figura 69). La primera se encarga de invocar este *software* primario, de la misma forma, provee del conjunto de instrucciones y modos de operación necesarios. La segunda, constituye en sí la programación para ejecutar el copiado de datos. Como ya se estableció previamente, este programa resulta conveniente cuando se presenten una o más de las siguientes condiciones:

1. Extracción total de datos contenidos en un DDE, disco lógico y/o unidad de almacenamiento masivo de datos.
2. Problemas identificados relacionados a la lectura y, por lo tanto, escritura de datos tales como: tratar de acceder a un archivo y notar un tiempo considerablemente superior al que se tomaba con anterioridad; de la misma forma, intenta realizar una extracción en aquellos volúmenes que, mediante la utilización del explorador de archivos, no sean accesibles por fallas lógicas, físicas y/o la combinación de estas pero que aún son identificados por el SO y/o el *software* “*diskmgmt.msc*”.

FERCUVILL V5.0 - MÓDULO 3: I.C.B.

BIENVENIDO USUARIO.

EJECUTE ESTE SOFTWARE PARA SALVAGUARDAR SU INFORMACIÓN EN UNIDADES DE ALMACENAMIENTO CON PROBLEMAS EN SU PROCESO DE LECTURA DE DATOS.

ATENCIÓN:

LEA LOS APARTADOS "FUNCIONES" E "INSTRUCCIONES" ANTES DE UTILIZAR EL MÓDULO.

FUNCIONES:

ESTE MÓDULO AVANZADO LE PERMITE REALIZAR UN PROCESO DE COPIADO MASIVO DE DATOS A PARTIR DEL USO DE UNA VENTANA EMERGENTE.

UTILICE ESTA HERRAMIENTA, PREFERENTEMENTE, PARA LOS SIGUIENTES PROPÓSITOS:

- RESPALDO DE INFORMACIÓN PARA UNIDADES DE ALMACENAMIENTO DE DATOS CON DETERIORO FÍSICO.
- RESPALDO TOTAL DE INFORMACIÓN DE UN DISCO LÓGICO.
- RECUPERACIÓN DE ARCHIVOS CON DETERIORO EN SU PROCESO DE LECTURA.
- EJECUTAR UNA MIGRACIÓN COMPLETA DE INFORMACIÓN MEDIANTE UN DISPOSITIVO EXTERNO.
- EN COMBINACIÓN CON UN PROCESO DE DESINFECCIÓN PREVIO, EJECUTAR UN RESPALDO PREVENTIVO.

INSTRUCCIONES:

- 1) PRESIONAR EL BOTÓN "INICIAR MÓDULO".
- 2) EN LA VENTANA SIGUIENTE, SEGUIR LAS INSTRUCCIONES ESPECIFICADAS.
- 3) NO CERRAR ESTA VENTANA, DE LO CONTRARIO, EL PROCESO DE COPIADO SERÁ INTERRUMPIDO.
- 4) ESPERAR A QUE LA EJECUCIÓN DEL MÓDULO SE COMPLETE.
- 5) UNA VEZ TERMINADO EL PROCESO, VERIFICAR QUE LA INFORMACIÓN SE ENCUENTRE EN LA RUTA ESPECIFICADA.
- 6) CERRAR LA VENTANA EMERGENTE Y DIRIGIRSE AL APARTADO "INFORMACIÓN ADICIONAL".

INFORMACIÓN ADICIONAL:

REINICIE EL EQUIPO INMEDIATAMENTE DESPUÉS DE COMPLETAR EL PROCESO DE COPIADO.

UTILICE EL "ASISTENTE AVANZADO DE INICIO". PRESIONE EL BOTÓN "MÓDULO 4. V.H.B.V." PARA TENER ACCESO A ESTE.

```
graph TD; B1[1] --> I[INICIAR MÓDULO]; B2[2] --> M4[MÓDULO 4: V.H.B.V.]; B3[3] --> M4;
```

Figura 68. Interfaz gráfica de operación para el MÓDULO 3: I. C. B.; visualización de “FUNCIONES” e “INSTRUCCIONES”.

Los elementos de la figura 68 son descritos a continuación en la tabla 41.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	EJECUTA EL <i>SOFTWARE</i> DE CONSOLA EXTERNA PARA EXTRACCIÓN DE DATOS.
2	MUESTRA EN PANTALLA EL <i>SOFTWARE</i> MEDULAR.
3	PERMITE APLICAR UN REINICIO AL SO MOSTRANDO EN PANTALLA EL ASISTENTE DEL MÓDULO 4: V. H. B. V.

Tabla 41. Descripción de los elementos estructurales del MÓDULO 3: I.C.B. del *software* “FERCUVILL V5.0”.

La consola de operación principal (figura 69) es mostrada una vez que se presiona el botón “INICIAR MÓDULO”, inmediatamente le solicitará al usuario la especificación del **DDE, disco lógico y/o unidades de almacenamiento masivo internos y/o externos que contengan la información a recuperar, así como la ruta exacta en formato de raíz (UNIDAD:) en la que esta será respaldada.** Citando nuevamente, los rangos de operación son los siguientes:

1. **DISCO_1**: Unidad de datos que contiene la información a ser recuperada.
2. **DISCO_2**: Unidades de almacenamiento dispuesta a contener la información recuperada.

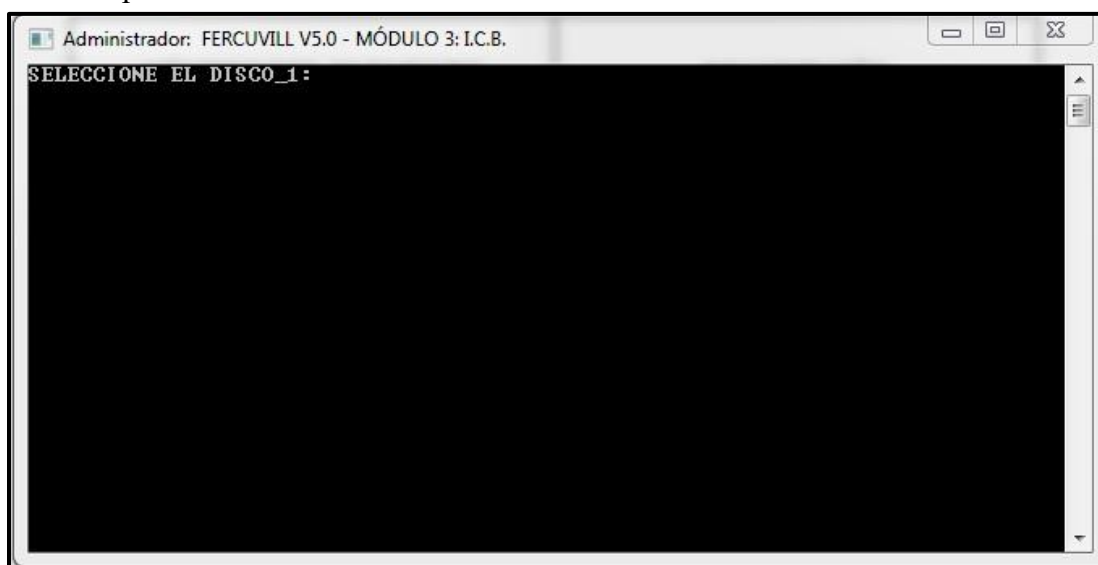


Figura 69. Interfaz de la consola externa principal del MÓDULO 3: I. C. B. para extracción de datos.

Los argumentos “DISCO_1” y “DISCO_2” son mutuamente excluyentes, es decir, de ser idénticos, el *software* no permitirá la ejecución alguna de instrucciones de programación.

Considérense las unidades lógicas “D:” y “G:” para ejemplificar su comportamiento. En el siguiente arreglo, “D:” se considerará como “DISCO_1”, en tanto que “G:” será “DISCO_2”.

1. Selección de la unidad “D:” como disco de datos a recuperar (colocar la letra, dos puntos verticales y presionar la tecla “ENTER”), (figura 70).

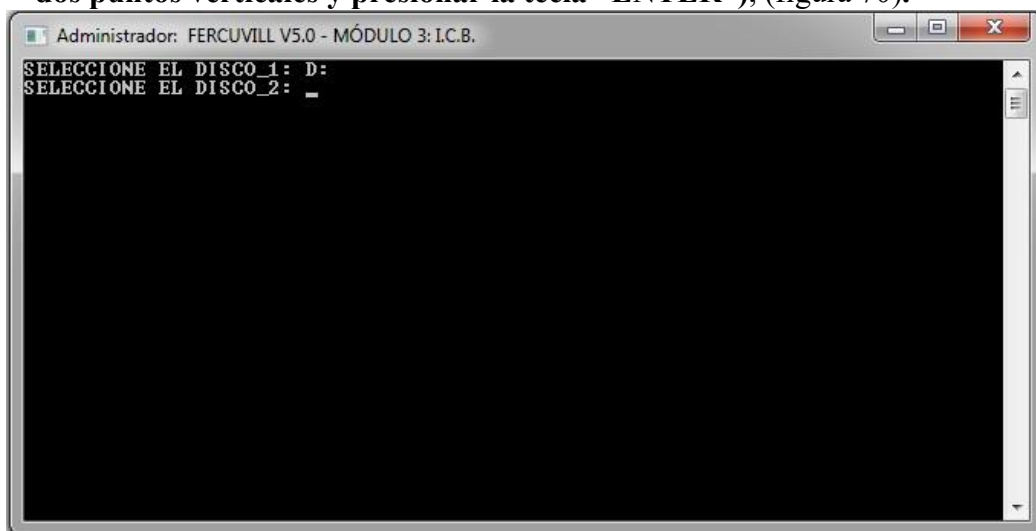


Figura 70. Selección del argumento “DISCO_1”.

2. Selección de la unidad “G:” como disco contenedor de datos (colocar la letra, dos puntos verticales y presionar la tecla “ENTER”), (figura 71).

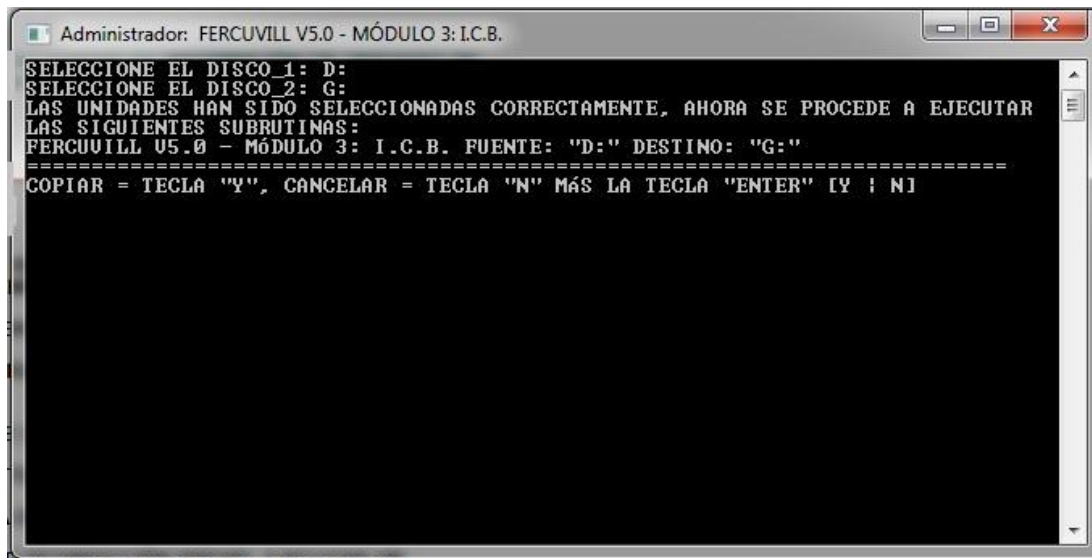


Figura 71. Selección del argumento “DISCO_2”.

El módulo ha identificado correctamente las unidades introducidas por el usuario, ahora sólo está esperando la confirmación por parte de este para proceder con la recuperación. Para dicho ejemplo, considérense ambas situaciones, en la primera de estas, el usuario acepta y, en la segunda, este cancela el procedimiento.

- 3. El usuario prosigue con la recuperación de datos:** para continuar, es necesario seguir las instrucciones mostradas en la consola, a cambio, el usuario recibirá el siguiente mensaje (figura 72):

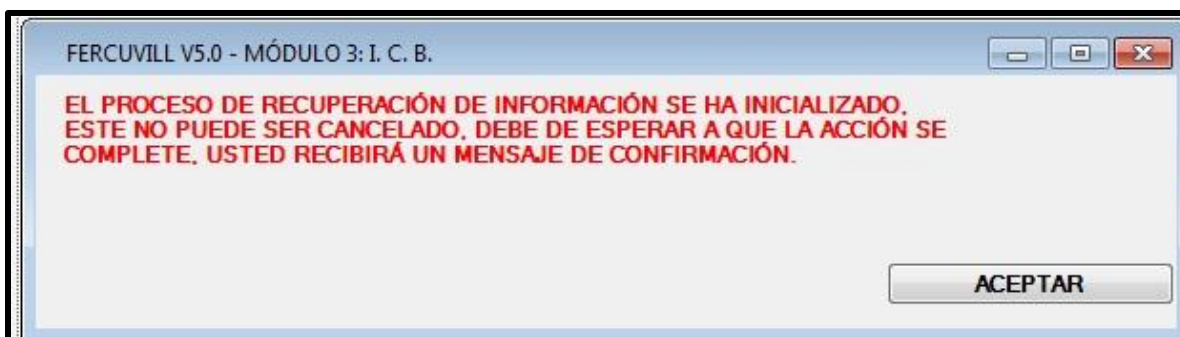


Figura 72. Mensaje del sistema (5): para el inicio del proceso de extracción de información.

Una vez finalizada la subrutina, el módulo mostrará un segundo mensaje en pantalla, tal y como se muestra a continuación (figura 73):

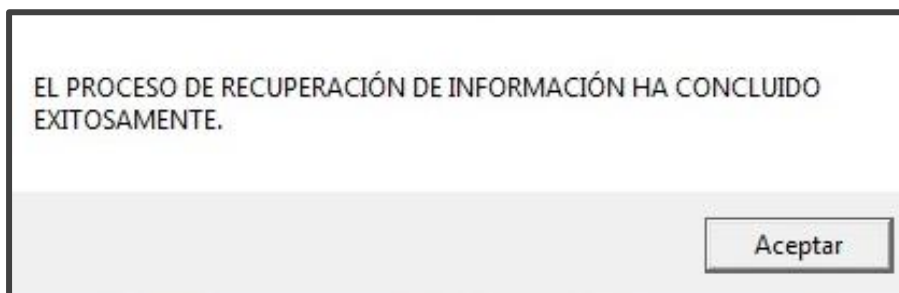


Figura 73. Mensaje del sistema (6): para la notificar la finalización del proceso de extracción de información.

Una vez ejecutada la operación, el usuario podrá dirigirse hacia la unidad (externa y/o interna) que contiene la información mediante el uso del explorador de archivos. Allí se encontrará la información intacta, con una alta integridad lógica y catalogada como recuperada.

Antes de establecer el comportamiento del módulo estudiado cuando se cancela la operación, es necesario contemplar aquella situación en la que existe el riesgo de una

corrupción de datos a causa de una selección incorrecta por parte del usuario para los argumentos “DISCO_1” y “DISCO_2”.

Considérese el caso en el que, tanto la unidad de “origen” como de “destino” son la misma, la información sería escrita en una misma dirección física y lógica sin generar duplicados, es decir, existiría una destrucción de los valores lógicos que conforman la estructura básica de la información.

Los módulos primarios contemplados en el presente proyecto de investigación, como ya se ha citado previamente, están contruidos para evitar y anular toda operación que atente de forma directa e indirecta a la información.

Como ejemplo práctico, se utilizará el disco lógico “G:” como valor único para los argumentos “DISCO_1” y “DISCO_2” (figura 74) y, mediante capturas de pantalla, se observará su comportamiento.

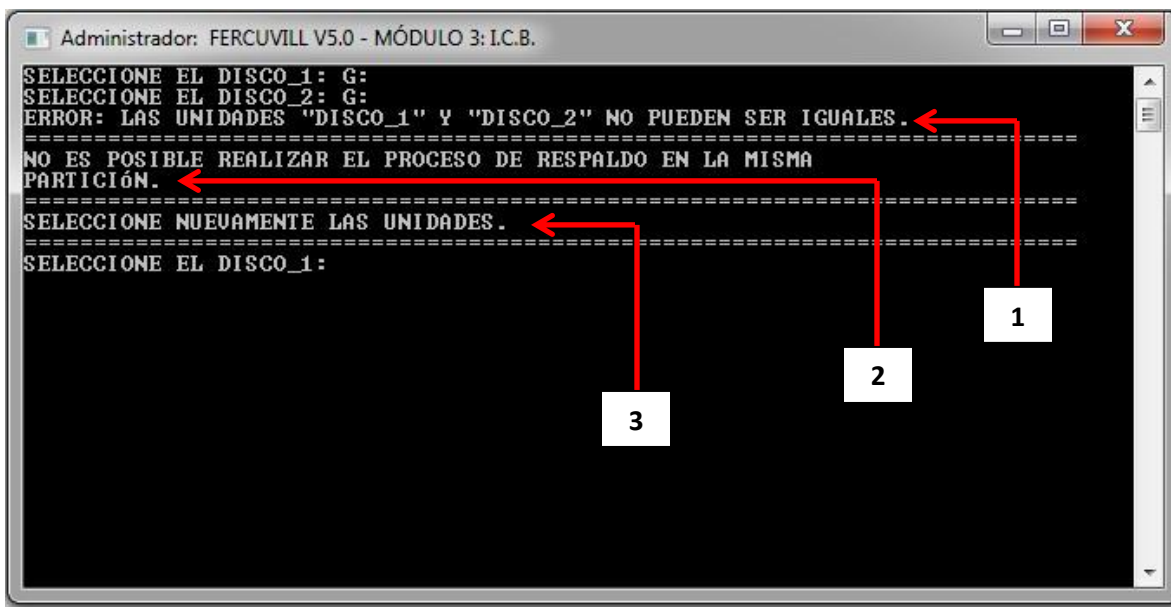


Figura 74. Selección del argumento “DISCO_1” y “DISCO_2” con el mismo valor (reiteración) y visualización del mensaje en el *software*.

De la figura anterior, es posible observar que el módulo, de forma inmediata, suprime todo intento del usuario por continuar con la operación, y en ese mismo instante, se le advierte la razón de ello. De forma complementaria, se le informa que debe de colocar correctamente las unidades lógicas para continuar con el proceso de recuperación de información.

Los elementos de la figura 74 son descritos a continuación en la tabla 42.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	SE LE INDICA AL USUARIO QUE HA COLOCADO LA MISMA UNIDAD DE “ORIGEN” Y DE “DESTINO”.
2	MUESTRA EN PANTALLA UNA EXPLICACIÓN SOBRE LA CONDICIÓN DESCRITA.
3	PERMITE COLOCAR NUEVAMENTE LAS UNIDADES SOLICITADAS SIN CERRAR LA APLICACIÓN DE CONSOLA.

Tabla 42. Comportamiento, mensajes y opciones de configuración para un caso de iteración en los parámetros “DISCO_1” y “DISCO_2”.

4. **El usuario no prosigue con la recuperación de datos:** para este escenario, el usuario ha decidido cancelar el procedimiento antes de ejecutarlo (figuras: 75 y 76), a cambio, se le mostrará la siguiente serie de mensajes en pantalla:

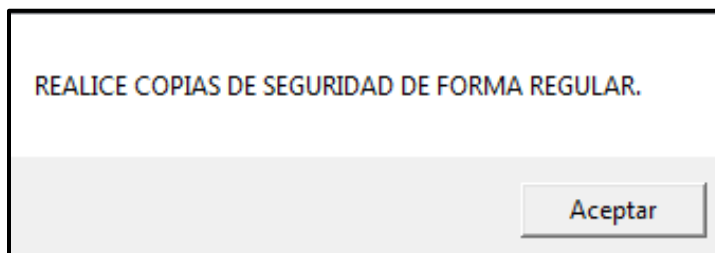


Figura 75. Mensaje del sistema (7): solicitud de respaldo.

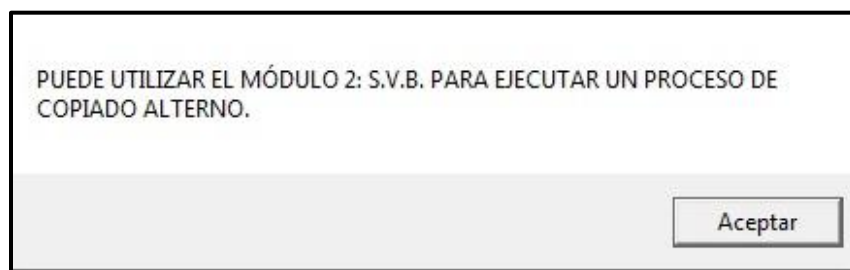


Figura 76. Mensaje del sistema (8): sugerencias de *software*.

Finalmente, la consola analizada se cerrará automáticamente, esta podrá ser invocada nuevamente desde la ventana gráfica del módulo estudiado (figura 68).

3.3.6 MÓDULO 4: V. H. B. V.

Este programa constituye una interfaz de control de procesos y administración directa de módulos (figura 77), como característica exclusiva, permite desencadenar subrutinas para iniciar, reiniciar y anular todos proceso relacionado al apagado del SO “huésped” de “FERCUVILL V5.0”. En adición, proporciona herramientas esenciales para el diagnóstico y evaluación de las características físicas y lógicas principales de un DDE en específico.

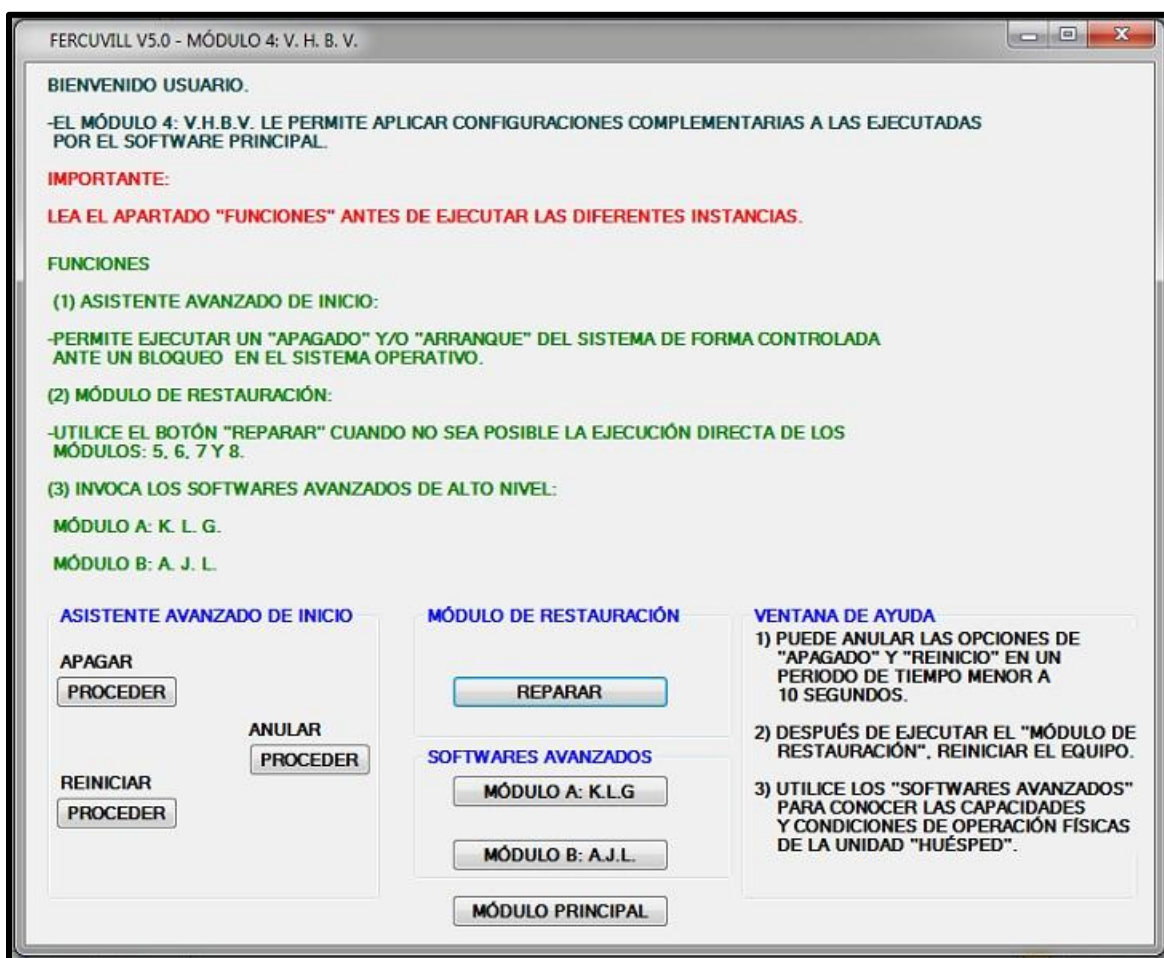


Figura 77. Interfaz gráfica de operación para el MÓDULO 4: V. H. B. V.; visualización de: “FUNCIONES”, “ASISTENTE AVANZADO DE INICIO”, “MÓDULOS DE RESTAURACIÓN”, “SOFTWARES AVANZADOS” y “VENTANA DE AYUDA”.

De forma complementaria a su utilización, ese módulo ha sido configurado para mostrar una sección de “ayuda”, la cual, se encuentra ubicada en la esquina inferior derecha de la

pantalla principal del mismo. A continuación, se procede a realizar la descripción de los elementos internos conformantes del módulo expuesto.

ASISTENTE AVANZADO DE INICIO

Esta sección del *software* permite la aplicación de un proceso de apagado, reinicio y/o la anulación de estos. Está diseñado para funcionar bajo las siguientes condiciones:

1. Hay tecnologías y procesos propios de “FERCUVILL V5.0” que necesitan de reiniciar el equipo computacional para que surtan efecto, de lo contrario, funcionarán de forma limitada y/o errática.
2. Existen programas maliciosos que, al intentar desactivar su funcionamiento (análisis por *software* “antivirus”) y/o extraer un objeto sobre el cual tengan influencia, ejecutarán de forma inadvertida una instrucción de reinicio, para ello se ha implementado una tecnología de anulación, de esa forma la eliminación del código vírico es posible y, por lo tanto, la recuperación de la información también.

El usuario sólo debe de seleccionar la opción deseada y, respectivamente, esta automáticamente se ejecutará, a cambio, este recibirá diferentes mensajes de confirmación para cada caso (figuras: 78, 79 y 80).

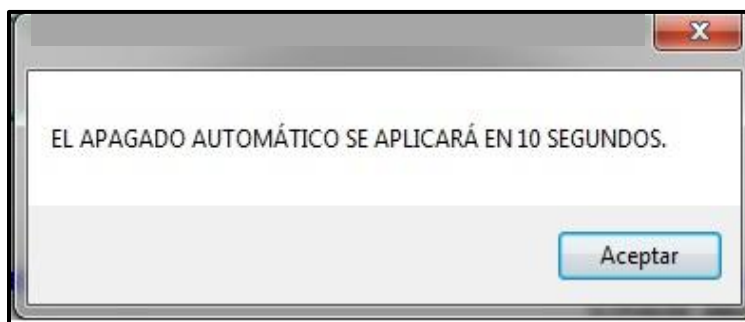


Figura 78. Mensaje del sistema (9): para advertir sobre el apagado del equipo.

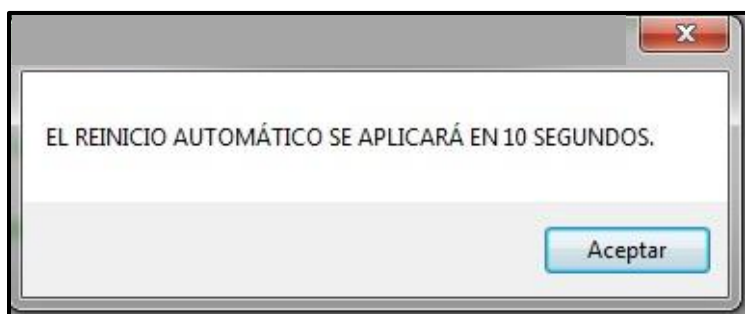


Figura 79. Mensaje del sistema (10): para advertir sobre el reinicio del equipo.

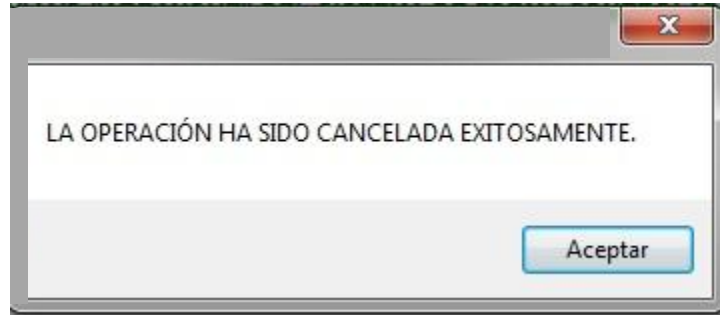


Figura 80. Mensaje del sistema (11): para anular un proceso de apagado/reinicio.

MÓDULO DE RESTAURACIÓN

Este es el encargado directo de la activación y/o desactivación de los módulos secundarios con los identificadores: 5, 6, 7 y 8. El usuario podrá decidir entre este par de opciones para ejecutar un proceso con mejores posibilidades de recuperación.

Esta tecnología está diseñada para cumplir con las siguientes funciones:

- Inhabilitar/Habilitar tecnologías que, debido a errores del SO y/o incompatibilidad con otras herramientas externas, puedan generar conflictos internos y ejecuciones incompletas de programas.
- Controlar el comportamiento de los módulos mencionados y, en combinación con otro *software* del tipo “antivirus”, permitir al SO eliminar objetos víricos sin comprometer la integridad de la información contenida y de “FERCUVIL V5.0” mismo.

Una vez el usuario seleccione esta opción, se le mostrará la siguiente ventana de operación (figura 81):

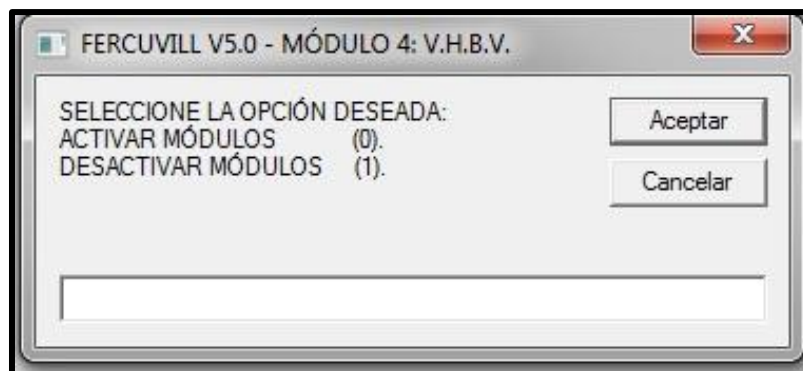


Figura 81. Ventana de operación del MÓDULO 4: V. H. B. V. para la consola de restauración.

De la figura 81, es posible observar que se contemplan solamente un par de opciones posibles, por lo tanto, se deberá seleccionar solamente entre estas, de lo contrario, el usuario recibirá el siguiente mensaje (figura 82):

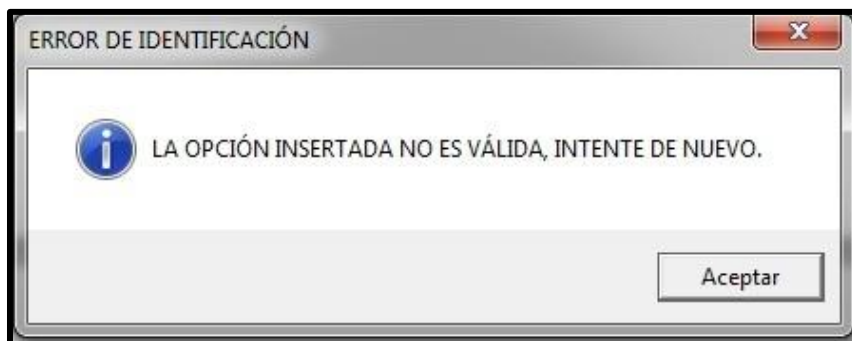


Figura 82. Mensaje del sistema (12): para un error en la solicitud de datos.

Ahora bien, de seleccionarse entre las opciones “0” y “1” respectivamente, este mismo usuario recibirá las siguientes respuestas e instrucciones a seguir (figuras 83 y 84), de no completar el proceso, la tecnología no estará disponible.

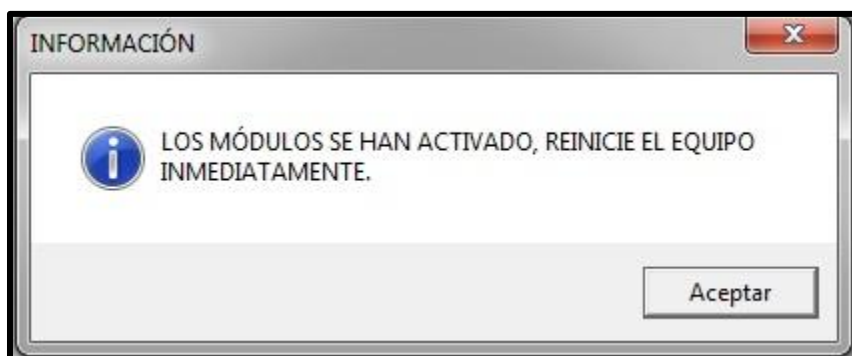


Figura 83. Mensaje del sistema (13): para indicar la activación de los módulos.

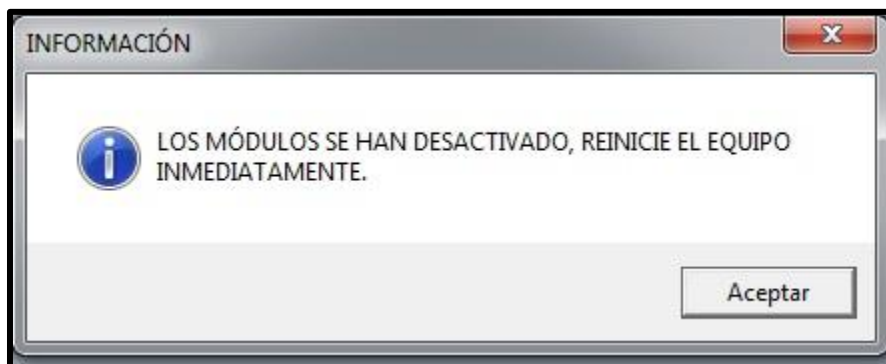


Figura 84. Mensaje del sistema (14): para indicar la desactivación de los módulos.

La utilización de este módulo no tiene restricción alguna, sin embargo, para cada cambio establecido el reinicio del sistema computacional es obligatorio.

SOFTWARES AVANZADOS

Esta sección contiene un par de programas orientados a la conservación física y lógica de la información contenida en un mismo DDE/volumen lógico respectivamente, mediante el análisis de los valores referentes a la integridad de la unidad y, en adición, al diseño de áreas aisladas para el depósito de datos.

3.3.7 MÓDULO A: K. L. G.

Este módulo le muestra al usuario información general y específica del DDE sobre el cual el *software* “FERCUVILL V5.0” se está ejecutando y, en función de dicha información, se puede definir si aplica o no el método de recuperación de datos propuesto (figura 85).

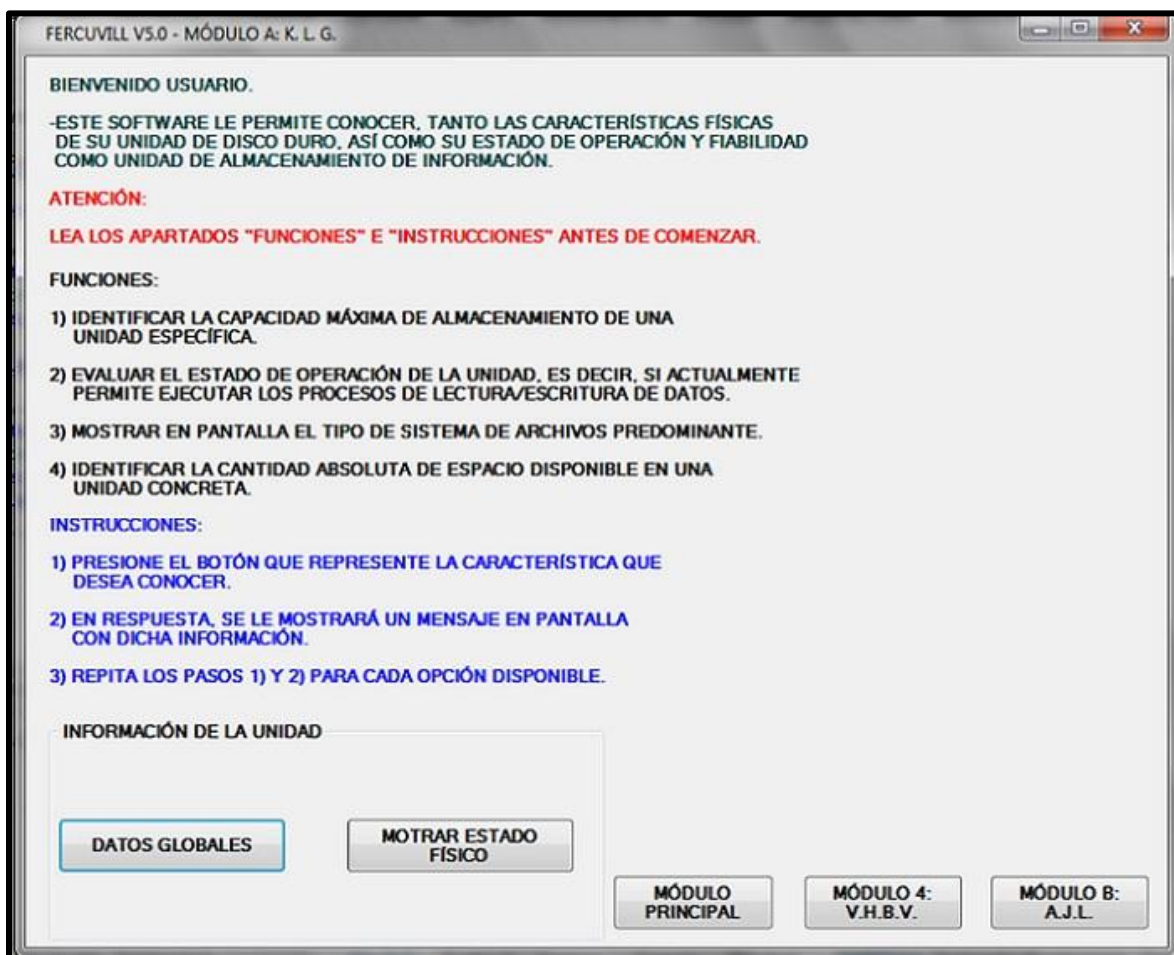


Figura 85. Interfaz gráfica de operación para el MÓDULO A: K. L. G.; visualización de “FUNCIONES”, “INSTRUCCIONES” e “INFORMACIÓN DE LA UNIDAD”.

Los valores y datos mostrados por este *software* serán dinámicos ya que dependen del equipo de cómputo, DDE y/o todos los elementos físicos y lógicos involucrados.

3.3.8 MÓDULO B: A. J. L.

Este *software* permite generar y/o proteger una ubicación segura en específico de acceso no autorizado por elementos del SO, usuarios y/o programas de código vírico dentro de un volumen. El usuario puede utilizar esta tecnología para ejecutar una restricción del acceso a la información de forma definitiva y completa (figura 86).

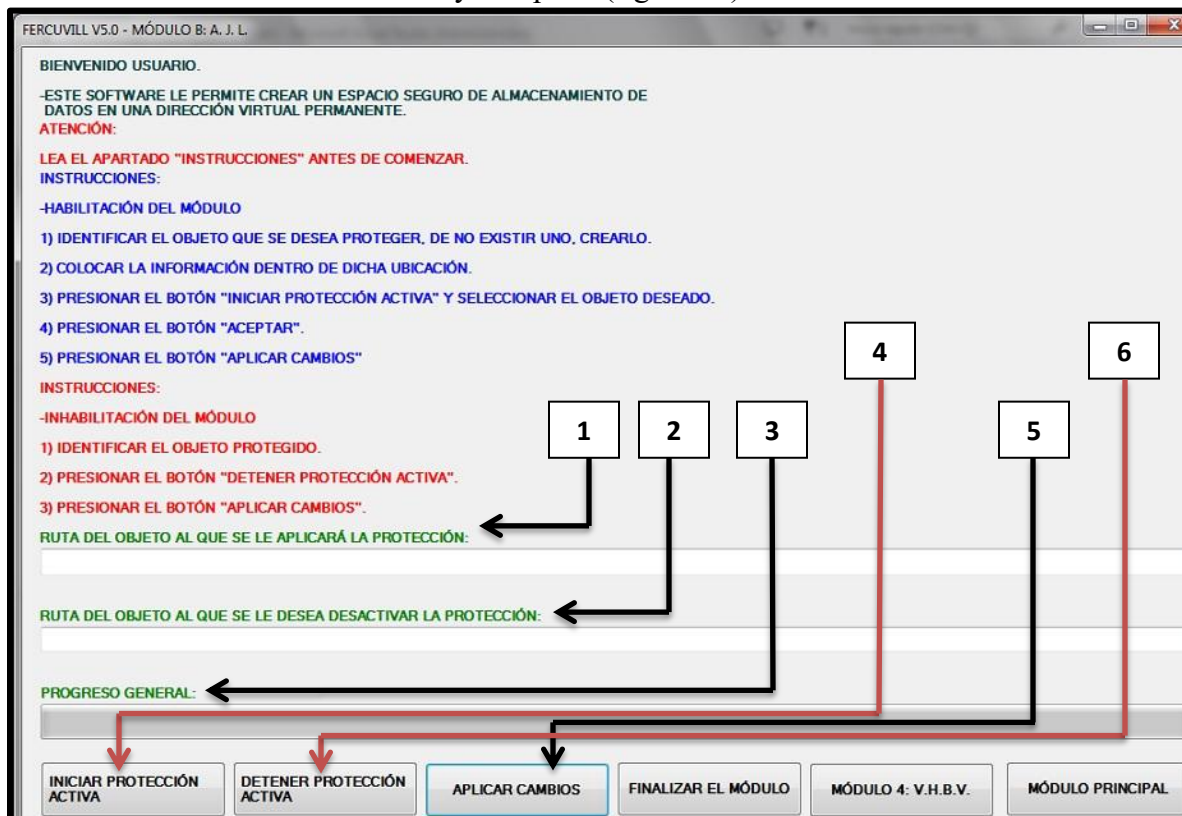


Figura 86. Interfaz gráfica de operación para el MÓDULO B: A. J. L.; visualización de “INSTRUCCIONES”, “RUTA DE LOS OBJETOS”, “PROGRESO GENERAL” y “BOTONES DE CONTROL”.

Es importante que el usuario conozca la dirección de SO en la cual se encuentra dicha protección activada (para identificar rápidamente la organización de los archivos y su contenido) y/o desactivada (para poder aplicar un proceso de edición y/o manipulación de los datos).

Los elementos de la figura 86 son descritos a continuación en la tabla 43.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	MUESTRA EN PANTALLA LA UBICACIÓN ESPECÍFICA DEL OBJETO AL QUE SE LE APLICARÁ LA TECNOLOGÍA.
2	MUESTRA EN PANTALLA LA UBICACIÓN ESPECÍFICA DEL OBJETO AL CUAL SE LE APLICARÁ UN PROCESO DE DESACTIVACIÓN DE LA TECNOLOGÍA.
3	PERMITE VISUALIZAR, MEDIANTE UNA BARRA DE ESTADO, EL AVANCE TOTAL DEL PROCESO EJECUTADO.
4	PERMITE ACTIVAR LA TECNOLOGÍA SOBRE UN OBJETO ESPECÍFICO Y/O CREADO POR EL USUARIO.
5	PERMITE GUARDAR LOS CAMBIOS EFECTUADOS (OBLIGATORIO).
6	PERMITE DESACTIVAR LA TECNOLOGÍA SOBRE UN OBJETO ESPECÍFICO Y/O CREADO POR EL USUARIO PREVIAMENTE.

Tabla 43. Descripción de los elementos estructurales del MÓDULO B: A. J. L. del *software* “FERCUVILL V5.0”.

Este módulo solamente puede operar sobre objetos tales que el usuario indique, más no de forma global y/o totalmente automatizada; así mismo, de activarse la tecnología, esta solamente puede ser revertida mediante la utilización del módulo mismo, **intentar aplicar otros métodos podría provocar una pérdida y/o corrupción de datos generalizada.**

El usuario podrá recibir el siguiente mensaje en pantalla (figura 87) cuando la aplicación de la protección se haya efectuado a algún objeto en particular (ya sea existente y/o creado):

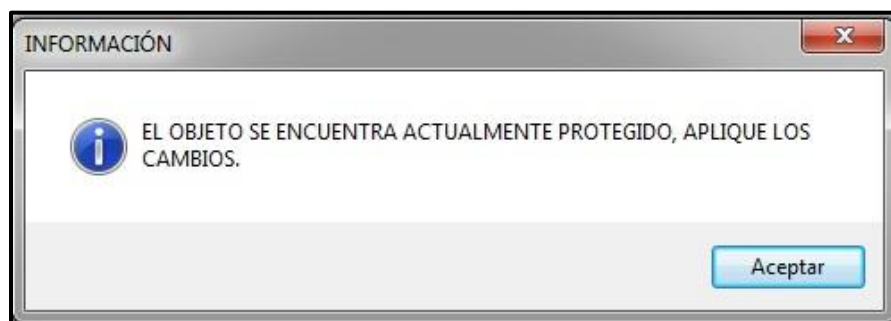


Figura 87. Mensaje del sistema (15): para un estado de protección activo de un objeto específico.

De forma contraria, cuando el usuario decida suspender la protección a un objeto previamente seleccionado, el siguiente mensaje de confirmación (figura 88) será mostrado:

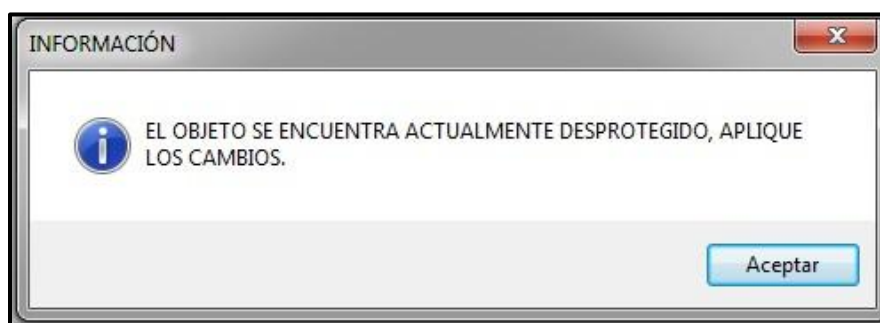


Figura 88. Mensaje del sistema (16): para un estado de protección inactivo de un objeto específico.

Indistintamente para la opción aplicada, es necesario que dichas modificaciones tomen efecto, por ello, existe una opción dentro del mismo módulo llamada “APLICAR CAMBIOS”, esta debe de ser seleccionada inmediatamente después de invocar cualesquiera de las posibles opciones mencionadas, de lo contrario, el objeto seguirá protegido y/o desprotegido, según corresponda.

3.3.9 MÓDULO 5: P. A. H.

La primera herramienta de este *software* le permitirá al usuario, mediante un SO, ejercer un nivel de configuración de pertenencia sobre un objeto (archivo y/o carpeta completos) tal que se encuentre vulnerado por la influencia de por una o más de las siguientes condiciones:

1. Agentes externos al SO (algoritmo vírico y/o programas inestables).
2. Eliminación de las propiedades de los archivos.
3. Deficiencias en la estructura del SO que impidan el cierre y/o ejecución de otras dependencias del mismo.

A continuación, en la figura 89, se muestra la ventana principal de operación de este módulo, nótese que existen botones de control para habilitar e inhabilitar la herramienta previamente descrita.

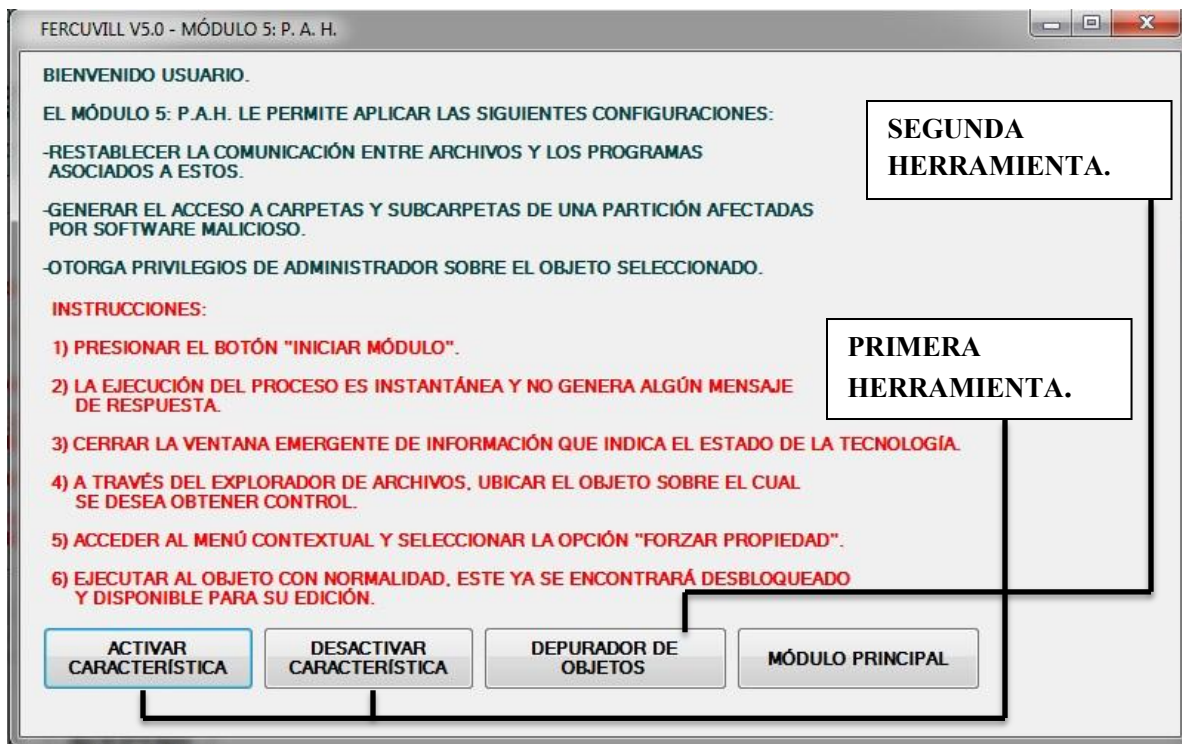


Figura 89. Interfaz gráfica de operación para el MÓDULO 5: P. A. H.; visualización de “INSTRUCCIONES”, “RUTA DE LOS OBJETOS”, “PROGRESO GENERAL” y “BOTONES DE CONTROL”.

Para el caso que corresponda, el usuario podrá aplicar múltiples veces los procesos de activación y desactivación mostrados en la figura anterior, pero para cada uno de estos,

existen mensajes en pantalla que indican su estado (figuras 90 y 91), los cuales, son esenciales para establecer el comportamiento del módulo estudiado.

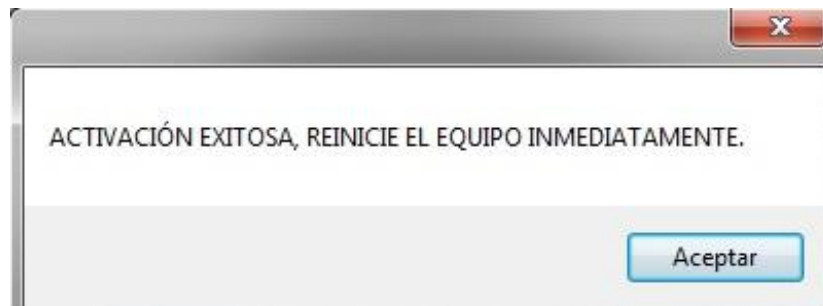


Figura 90. Mensaje del sistema (17): para la activación completa de la herramienta seleccionada.

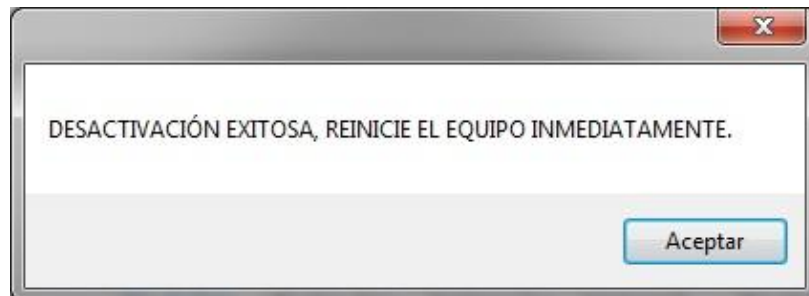


Figura 91. Mensaje del sistema (18): para la desactivación completa de la herramienta seleccionada.

Existe una segunda herramienta nativa de este módulo, la cual, tiene como objetivo principal el restablecimiento a sus valores de inicio de cualquier *software* instalado en el SO.

Los archivos generados por los programas asociados están sujetos a ser “apropiados” por estos cuando, por razones varias, el mismo *software* no es capaz de desencadenar una serie de comandos para “desprenderse” de ellos; por lo tanto, y puesto que el elemento se encuentra todo el tiempo bajo el control del programa inestable, la extracción del datos no es posible.

Esta herramienta, a continuación expuesta, brinda la posibilidad de recuperar los archivos hasta el último evento registrado en el cual fueron guardados y, con ello, todas las modificaciones aplicadas, o bien, la última versión consistente que no se encontraba bloqueada por dicho *software* (figura 92).

Así mismo, la participación de virus informáticos puede ocasionar que la información sea temporal o permanentemente inaccesible; esto debido a que el algoritmo malicioso forzará al elemento a estar perpetuamente ejecutado (imposibilitando así su manipulación/adición). Es entonces cuando esta herramienta (“DEPURADOR”) detendrá la ejecución global de los objetos y, posteriormente, admitirá solamente la del archivo en cuestión, permitiendo así su cierre y respectivo proceso de extracción.

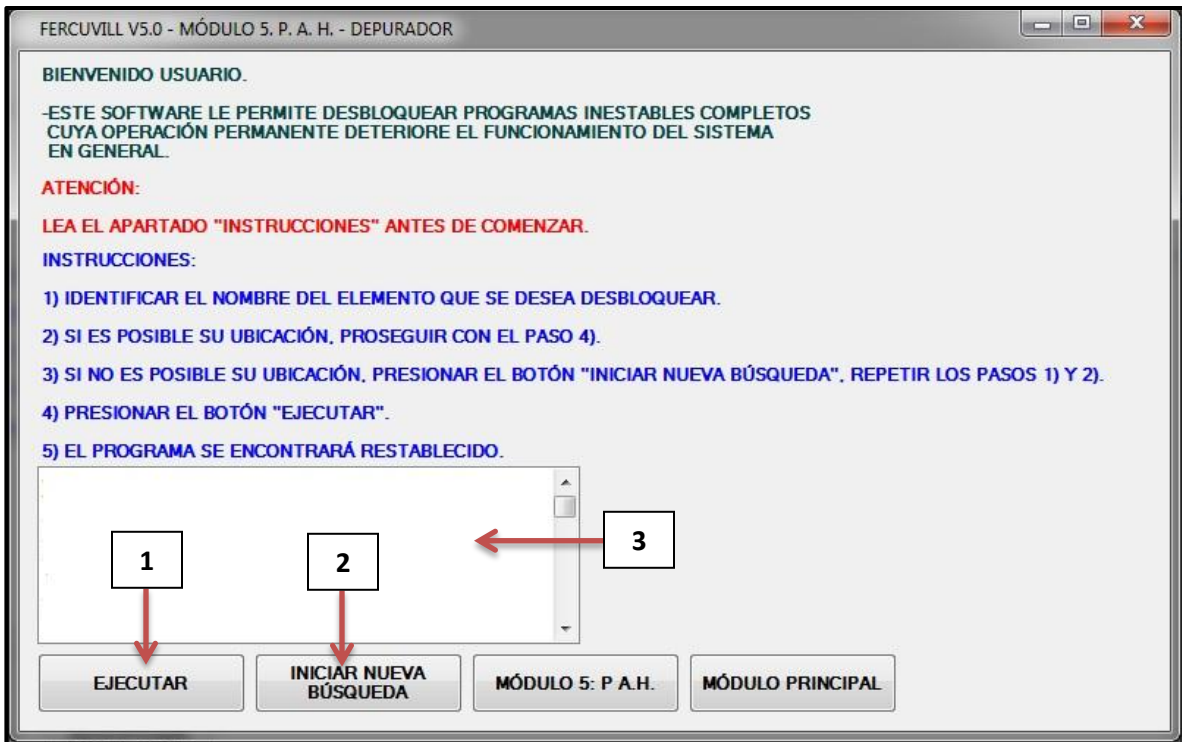


Figura 92. Interfaz gráfica de operación del MÓDULO 5: P. A. H. para la ejecución del *software* “DEPURADOR”.

El usuario deberá de identificar el nombre (e incluso nombres) referido a cada uno de los posibles programas involucrados en la ejecución de su información, solamente deberán ser desbloqueados aquellos relacionados directamente. Esta tecnología (**recursiva**) está en contacto directo con otros *softwares* internos y externos al SO, por lo tanto, la alteración irresponsable y/o sin conocimiento de dichas estructuras podrá, potencialmente, destruir el ambiente de operación en donde reside la información del usuario.

Si, aún después de presionar el botón llamado “INICIAR NUEVA BÚSQUEDA”, la identificación es parcial y/o no se ha solucionado el problema original de bloqueo, es preferible realizar un proceso forzado de recuperación de información integral, el cual, está contemplado actualmente dentro de las características de extracción de datos por el

MÓDULO 3: I. C. B.; de esa forma, los programas internos al SO y/o los algoritmos maliciosos persistentes serán (mayoritariamente) desactivados, pues, existirá otro ambiente no nativo de SO el cual podrá editar y desinfectar la información recuperada.

Los elementos de la figura 92 son descritos a continuación en la tabla 44.

NÚMERO DEL ELEMENTO	DESCRIPCIÓN
1	DESENCADENA LA SERIE DE COMANDOS NECESARIOS PARA FORZAR EL DESBLOQUEO DE UN PROGRAMA ESPECÍFICO.
2	APLICA UN ALGORITMO AVANZADO DE IDENTIFICACIÓN DE PROGRAMAS EJECUTADOS EN PRIMER Y SEGUNDO PLANO, ASÍ MISMO, MUESTRA LOS RESULTADOS EN PANTALLA.
3	PERMITE VISUALIZAR, MEDIANTE UNA UN ESPACIO DE TEXTO SIMPLE, LA LISTA DE PROGRAMAS ENCONTRADOS.

Tabla 44. Descripción de los elementos estructurales del MÓDULO 5: P. A. H. para la ejecución del *software* “DEPURADOR”.

3.3.9.1 MÓDULO 6: S. H. B. V.

Este módulo establecerá un patrón de protección ante programas víricos para dispositivos de almacenamiento de información del tipo no volátil de interfaz USB, si y sólo si, estos elementos son del tipo “re-escribibles” (exclúyase a las unidades de CD/DVD externas).

Puesto que la información contenida en un sistema computacional local es, frecuentemente, recibida, transmitida y/o compartida a través de memorias digitales de interfaz USB, y en adición, se ha estudiado que este medio es uno de los más prolíferos para la propagación efectiva de aplicaciones víricas y algoritmos maliciosos; el *software* “FERCUVILL V5.0”

instala una tecnología de protección en tiempo real, para así, contener la infección, la cual, anula la capacidad de los virus informáticos internos de un SO para asirse a memorias digitales y, de esa forma, contener la infección.

Es importante enfatizar que “FERCUVILL V5.0” no es un *software* de protección “antivirus”, (pues no cuenta con las características descritas en la páginas 109 y 110 del presente capitulado) sin embargo, este se define como uno de recuperación de información y, en concordancia con lo establecido previamente, se deben de generar márgenes de extracción de datos aceptables; por ello, el programa diseñado está dotado con una tecnología para la anulación del proceso infeccioso de ciertas amenazas, las cuales, explotan dicha vía de comunicación mencionada.

El ambiente gráfico de operación (figura 93) del módulo estudiado presenta las opciones para instalar y/o desinstalar la tecnología de protección de datos; el usuario podrá ejecutar de forma indiscriminada dichas opciones según corresponda su necesidad y nivel de seguridad.

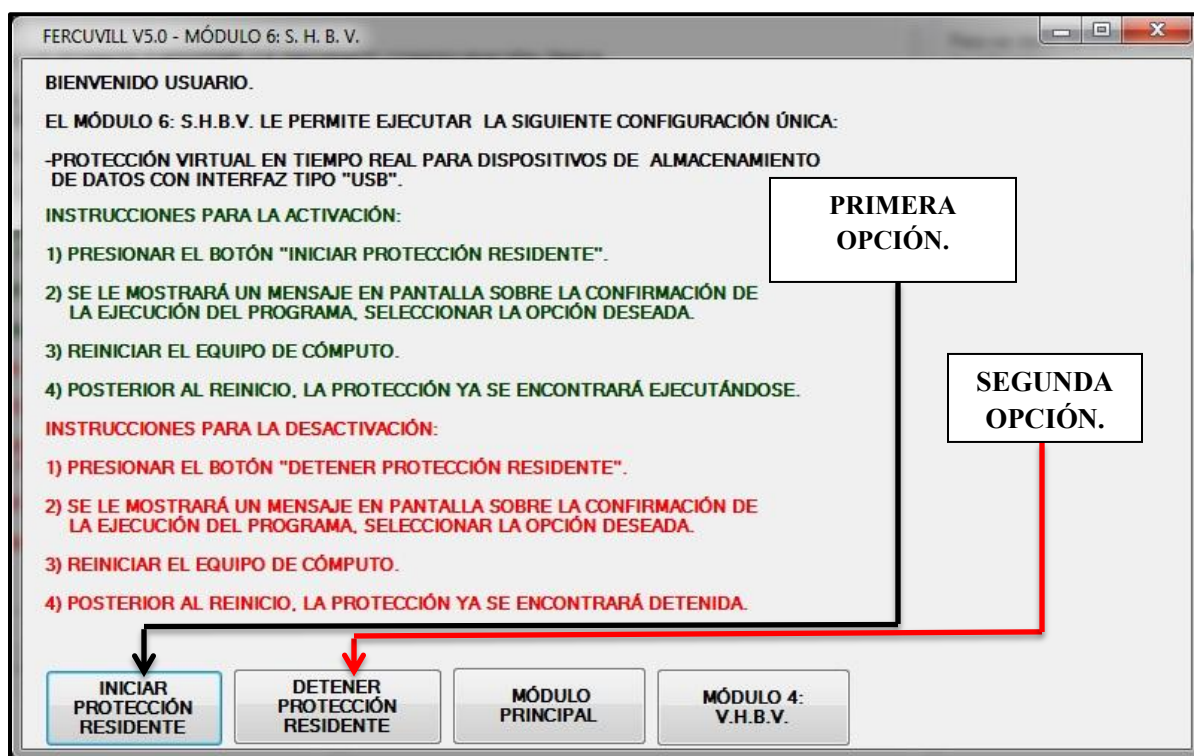


Figura 93. Interfaz gráfica de operación para el MÓDULO 6: S. H. B. V.

Esta tecnología está prevista con un algoritmo para forzar su aplicación en el SO “huésped” independientemente de las condiciones en las que este se encuentre (siempre y cuando el SO sea capaz de iniciar y reconocer al DDE y, por lo tanto, las particiones y dispositivos externos de datos), de tal forma que, de existir la información suficiente el programa se ejecutará de forma regular, para el caso contrario, construirá dichas estructurales temporales para que se permita su instalación.

Se observa, de la figura 94, que solamente existen un par de posibles opciones de ejecución para el *software*, pero para cualesquiera que el usuario seleccione, este siempre recibirá el siguiente mensaje de confirmación (figura 94):

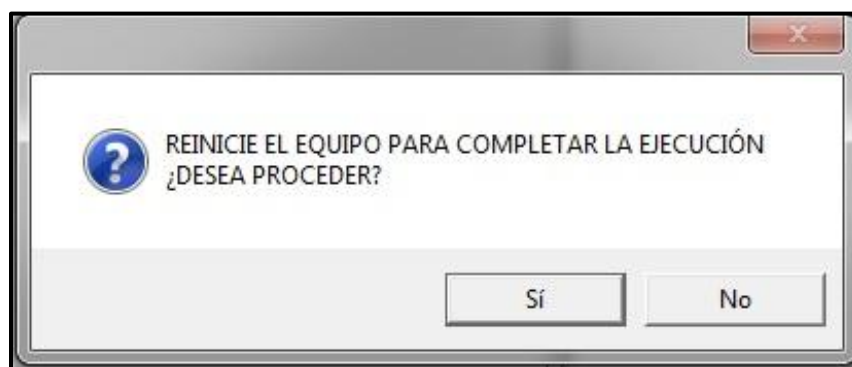


Figura 94. Mensaje del sistema (19): solicitud de continuación y reinicio del sistema.

Después de completar la ejecución, el mismo módulo le ofrecerá al usuario (figura 95) la opción de invocar un reinicio especial del sistema computacional a partir de la herramienta expuesta en el MÓDULO 4: V. H. B. V.; este último proceso es crucial, pues, de no realizarse, el sistema comenzaría a operar de forma inestable y la protección sería parcial.

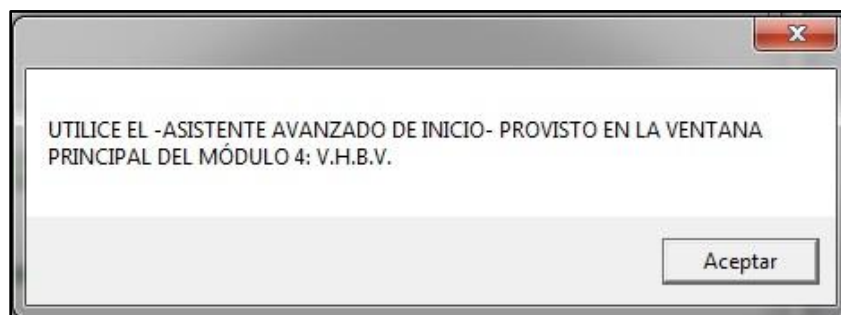


Figura 95. Mensaje del sistema (20): sugerencia de reinicio del sistema.

Completados los procesos de instalación y reinicio, la tecnología se encontrará (según corresponda) activada o desactivada. Para el primer caso, el usuario tendrá la posibilidad de acceder y editar la información contenida en el medio extraíble de datos, pero con el

resguardo de que su dispositivo no será infectado por las amenazas existentes en el equipo computacional al que se encuentre conectado. Para el segundo caso, la edición y manipulación también se encontrarán presentes, sin embargo, no existirán medios y/o tecnologías que prevengan al equipo computacional de infectar a los medios externos de almacenamiento de datos.

3.3.9.2 MÓDULO 7: H. A. A. B.

Este programa reúne múltiples tecnologías de control de datos para efectuar una correcta visualización, programación y, por lo tanto, extracción de datos en conjunto con los demás módulos propuestos.

La organización de herramientas en este módulo es a partir de la utilización de una ventana gráfica en la que, a través de una serie de comandos, se invoca otra del tipo emergente, la cual a su vez, es la encargada de desencadenar la secuencia de instrucciones lógicas allí establecidas.

A continuación, en la figura 96, se observa la interfaz gráfica de operación, al igual que el conjunto de instrucciones propias para el módulo expuesto:

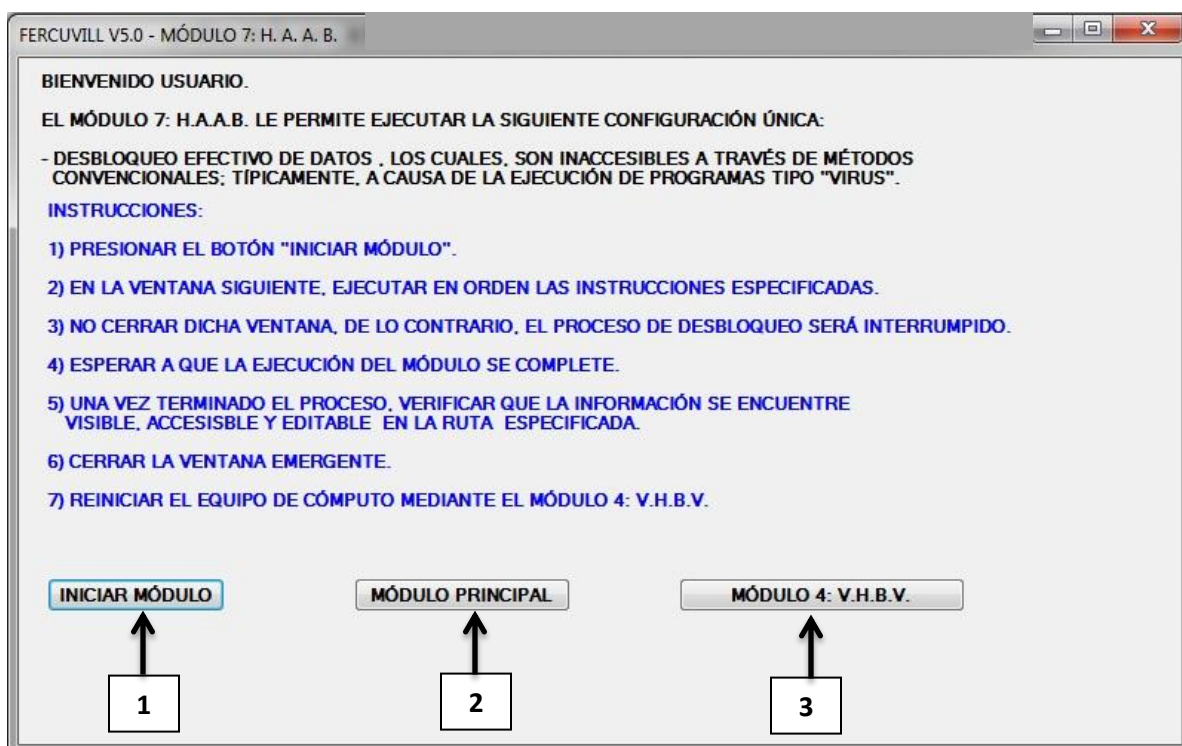


Figura 96. Interfaz gráfica de operación para el MÓDULO 7: H. A. A. B., visualización de elementos.

Para poder utilizar el *software* de forma correcta, el usuario debe de seleccionar la opción llamada “INICIAR MÓDULO”, una vez realizada esta operación, el mismo usuario observará la nueva ventana emergente (figura 97) y podrá aplicar las herramientas allí propuestas.

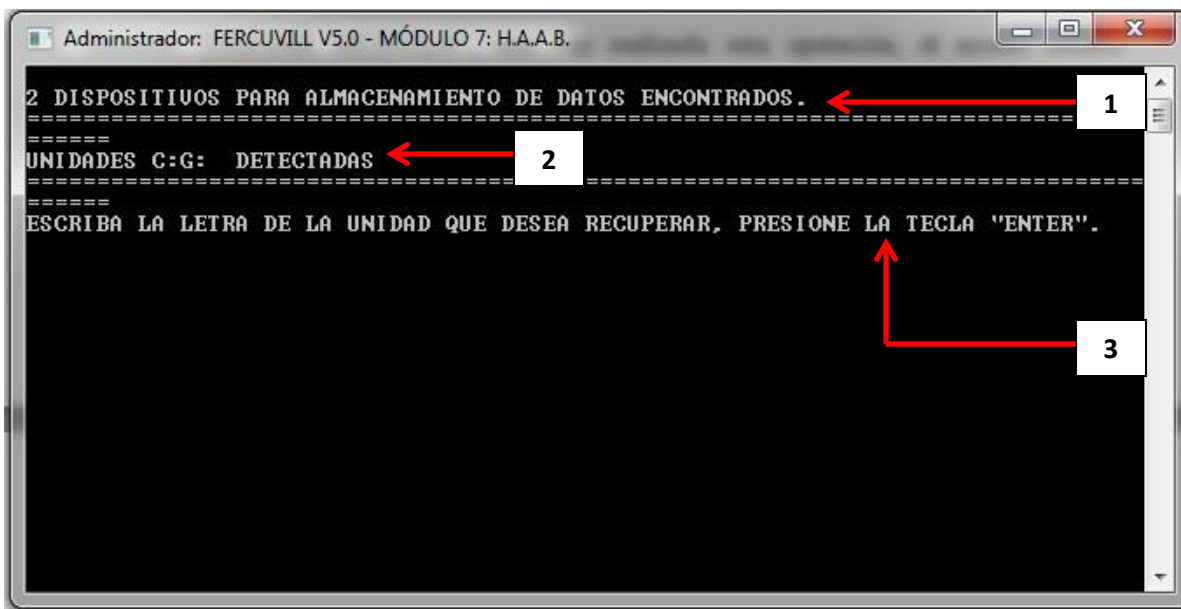


Figura 97. Interfaz de la consola externa principal del MÓDULO 7: H. A. A B. para el desbloqueo de datos.

A continuación, los elementos mencionados en las figuras 96 y 97 son descritos, respectivamente, en la tabla 45.

VENTANA DE INTERFÁZ GRÁFICA	DESCRIPCIÓN
1	PERMITE INVOCAR EL PROGRAMA PARA EL DESBLOQUEO DE INFORMACIÓN.
2	MUESTRA LA INTERFAZ PRINCIPAL DEL <i>SOFTWARE</i> “FERCUVILL V5.0”.
3	PERMITE AL USUARIO EL ACCESO DIRECTO AL MÓDULO 4:V.H.B.V.

VENTANA DE CONSOLA EXTERNA	DESCRIPCIÓN
1	INDICA AL USUARIO LA CANTIDAD DE VOLÚMENES LÓGICOS POSIBLES A SER MODIFICADOS POR EL PROGRAMA.
2	MUESTRA EN PANTALLA EL IDENTIFICADOR (LETRA) ASIGNADO A CADA DISCO LÓGICO QUE, POTENCIALMENTE, PUEDE SER SELECCIONADO.
3	SOLICITA DIRECTAMENTE AL USUARIO QUE ESPECIFIQUE EL CAMPO REQUERIDO PARA PROCEDER CON LA EJECUCIÓN DEL MÓDULO 7: H. A. A. B.

Tabla 45. Descripción de los elementos estructurales del MÓDULO 7: H. A. A. B. (interfaz gráfica y consola externa de operación) del *software* “FERCUVILL V5.0”.

Este módulo mostrará los siguientes mensajes informativos en pantalla una vez la consola externa sea ejecutada (figuras: 98, 99, 100 y 101, respectivamente).

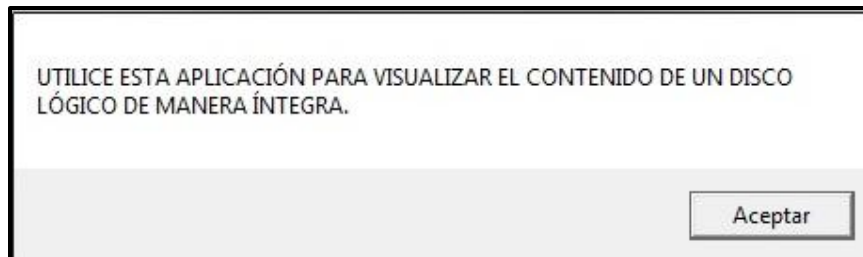


Figura 98. Mensaje del sistema (21): para visualizar íntegramente el contenido de un disco lógico.

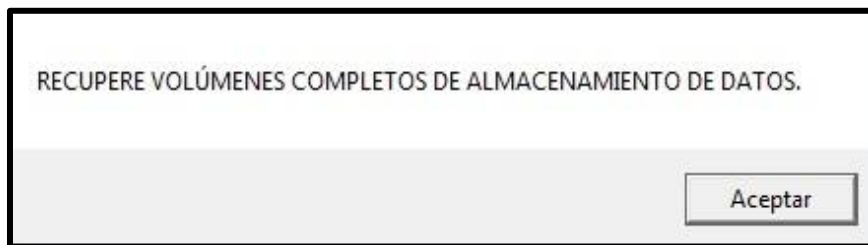


Figura 99. Mensaje del sistema (22): para la recuperación de volúmenes completos de datos.

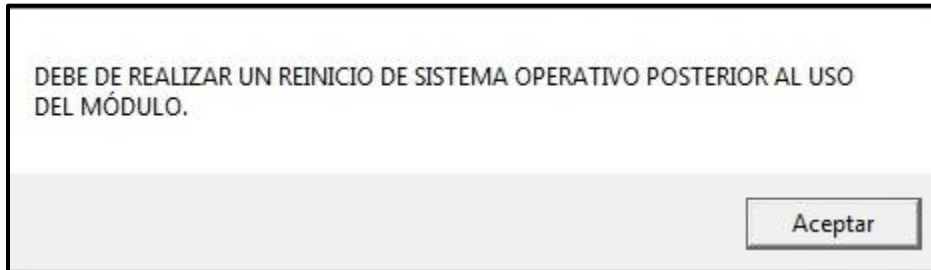


Figura 100. Mensaje del sistema (23): para le ejecución de un reinicio del sistema.

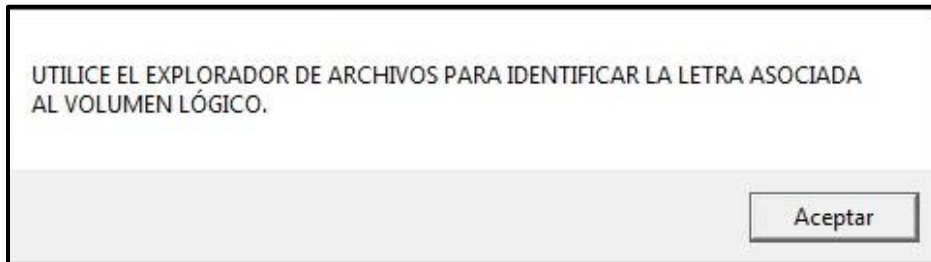


Figura 101. Mensaje del sistema (24): para visualizar le letra asociada al volumen lógico.

Se planteará un escenario, en el cual, se seleccionará una unidad lógica perteneciente a un DDE externo conectado a través de su interfaz tipo SATA. Se observa, de la figura 103, que la única serie posible de unidades lógicas a seleccionar son “C:”, “D:” y “G:”, siendo “D:” aquella asignada a una partición nativa de un DDE externo.

1. **Estableciendo el argumento “D:” en la consola.** Es necesario colocar el campo requerido, seguirlo de un par de puntos verticales y presionar la tecla “ENTER” (figura 102).

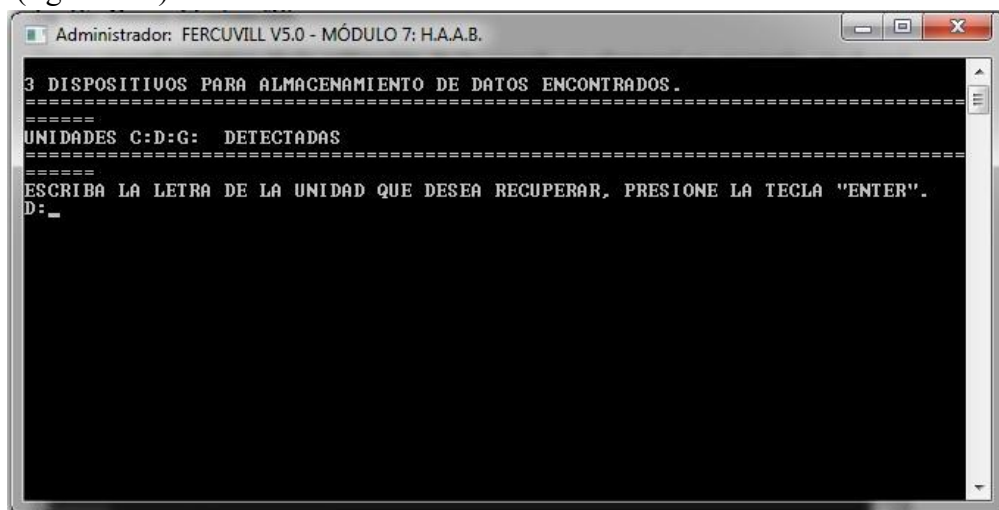


Figura 102. Selección de la unidad lógica descrita por el argumento “D:” como aquella a ser modificada por la consola externa.

El punto anterior es crucial, pues, el usuario debe de estar completamente seguro de que ha seleccionado la unidad correcta, de lo contrario, estaría modificando otra dirección lógica y, con ello, el proceso de desbloqueo de información sería (igualmente) infructífero.

- 2. Operación de la consola.** En esta etapa, dependiendo de la extensión (tamaño) de la unidad seleccionada, el algoritmo recorrerá cada localidad posible (a una determinada velocidad de lectura y escritura) en la unidad seleccionada, recuperando y restableciendo el acceso a la información contenida (figura 103).

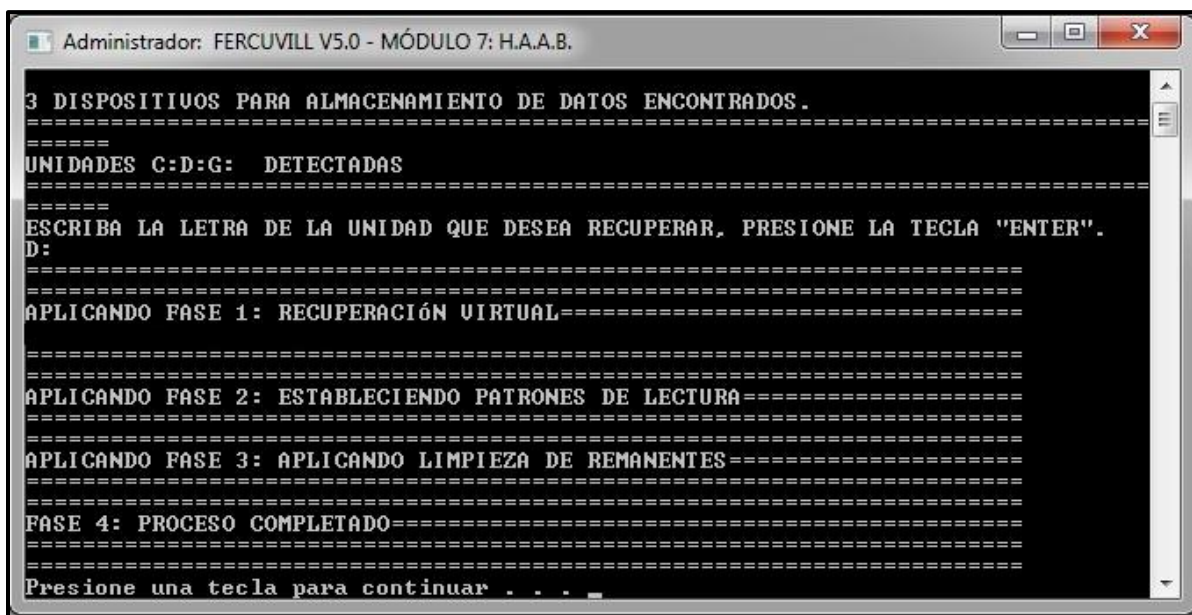


Figura 103. Ejecución de las etapas de desbloqueo de información sobre el objeto especificado como “D:” mediante la utilización de la consola externa.

Finalizado este procedimiento, el usuario podrá acceder a su información de forma segura. El *software* mismo indicará, mediante una serie de mensajes en pantalla, los pasos a seguir para extraer (figuras: 104, 105 y 106) de forma, preferentemente inmediata, la información a partir de la utilización de las herramientas propuestas en “FERCUVILL V5.0” (“MÓDULO 2: S. V. B.” y/o “MÓDULO 3: I. C. B.”).

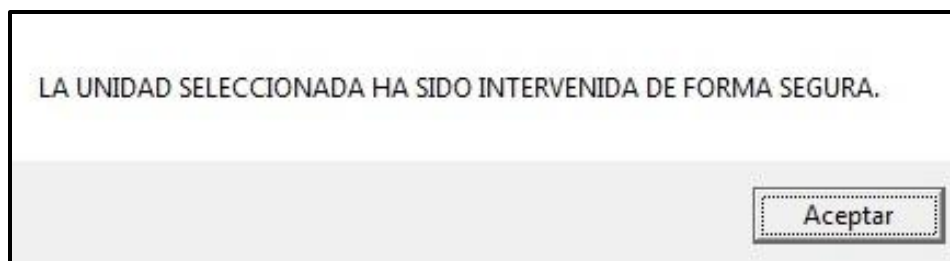


Figura 104. Mensaje del sistema (25): notifica la intervención segura del disco lógico analizado.

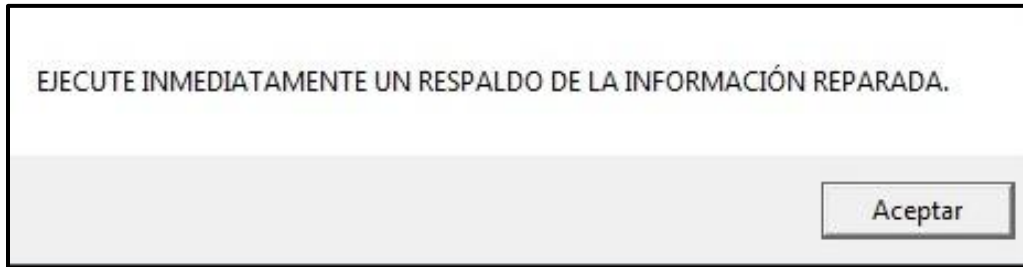


Figura 105. Mensaje del sistema (26): para ejecutar un respaldo de la información reparada.

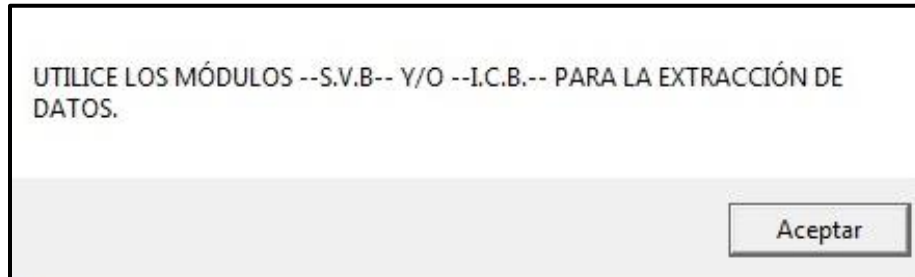


Figura 106. Mensaje del sistema (27): sugerencia para la extracción de datos.

- 3. Especificación incorrecta de los argumentos.** Como ejemplo práctico (y considerando las unidades expresadas en la figura 102) se colocará un argumento inexistente y, por lo tanto, indetectable por el *software* mismo (unidad "H:"); así mismo, se observará el comportamiento y respectivo mensaje del sistema (figura 107).

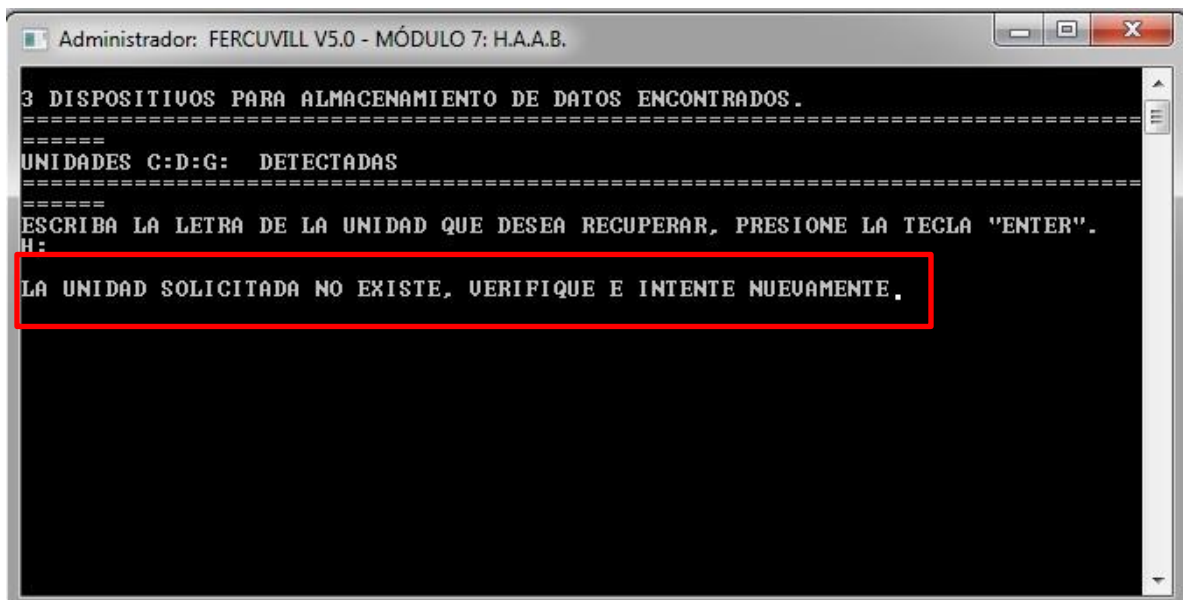


Figura 107. Selección del argumento "H:" como unidad de destino (inexistente) y visualización del mensaje en *software*.

De esta forma, se garantiza que el programa no operará en localidades aleatorias, así mismo, tampoco modificará otros elementos, pues, es capaz de identificar las unidades disponibles de un SO.

Finalmente, “FERCUVILL V5.0” podrá ser finalizado de forma segura, al igual que sus diferentes módulos, presionando los diferentes botones de control localizados en la esquina superior derecha para cada una de las ventanas de interfaz gráfica y/o de consola externa de operación.

CONCLUSIONES PARCIALES.

En este capítulo se estudió a “FERCUVILL V5.0” como aquel *software* programado para la recuperación de información en unidades de DDE a partir del análisis de sus respectivas representaciones virtuales (discos lógicos). Así pues, se examinaron sus estructuras y estratificaciones a partir de módulos de operación independientes y coordinados mediante parámetros de control programables y ejecutados en un ambiente físico (*hardware*) y lógico (*software*) de SO compatibles con las unidades físicas estudiadas.

Capítulo 4. MÉTODO PARA LA RECUPERACIÓN DE INFORMACIÓN EN DISCOS DUROS ELECTROMECÁNICOS MEDIANTE EL *SOFTWARE* “FERCUVILL V5.0”.

En este capítulo se expondrá el método propuesto orientado a la recuperación de datos en unidades de DDE; el cual, se desarrolla a partir de procedimientos generales efectuando un tratamiento (principalmente) lógico a estas unidades de almacenamiento de información. Este proceso de recuperación está basado y fundamentado por el *software* desarrollado en el presente proyecto de investigación: “FERCUVILL V5.0”. Así mismo, se analizarán escenarios reales de pérdida y restauración de información en objetos de estudio específicos (propuestos previamente) para evaluar/comprobar la efectividad (información recuperada) que el *software* mencionado tendrá sobre dichos objetos mediante una intervención directa aplicada a los archivos contenidos en el volumen lógico.

4.1 FASES DEL MÉTODO Y SU DESCRIPCIÓN

El procedimiento descrito previamente estará constituido por los siguientes campos:

- **FASE 1: PRESENTACIÓN DEL OBJETO ANALIZADO.**
- **FASE 2: IDENTIFICACIÓN DEL TIPO DE FALLA PREDOMINANTE.**
- **FASE 3: ANÁLISIS SOBRE LA VIABILIDAD DE LA UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0”.**
- **FASE 4: UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0” (MÓDULOS ESPECÍFICOS).**
- **FASE 5: COMPROBACIÓN Y ANÁLISIS DE RESULTADOS.**

OBSERVACIONES:

Las etapas (fases) anteriormente expresadas son universales exclusivamente para la utilización y ejecución del *software* “FERCUVILL V5.0”, no deben de ser consideradas así para otros métodos de recuperación de información, los cuales, pueden contener etapas de análisis lógico y/o físicos extensivas y específicas no aplicables para el método aquí expuesto.

DESCRIPCIÓN DE LAS FASES CONSTITUTIVAS

A continuación, se presenta la explicación y organización de las fases previamente citadas, así mismo, se especifican las características y contenidos propios de cada una de estas.

4.1.1 FASE 1: PRESENTACIÓN DEL OBJETO ANALIZADO

En esta sección, se estudian y mencionan las características físicas y lógicas (verificables) pertenecientes a las unidades de almacenamiento de datos que serán sometidas al método de recuperación de información expuesto.

Para el caso de las características lógicas, estas no pueden ser obtenidas en todos los casos pues, como ya se ha conceptualizado previamente, esta información depende, básicamente, de los parámetros de control establecidos en las siguientes estructuras:

1. *Software “firmware”* (existente en los platos magnetizables y en la memoria tipo ROM de la TCI).
2. Disponibilidad y estado de operación/acceso del AS y el AU asociados el DDE.
3. Disponibilidad y estado de operación/acceso al SA asociado al SO instalado en el disco lógico.
4. Características del disco y/o discos lógicos existentes en el dispositivo físico y/o dinámico.
5. Estado de operación: detectable o indetectable por el *software* BIOS.

Cuando existan condiciones de corrupción en cualquiera de las estructuras mencionadas, la información del estado lógico de la unidad estará comprometida y podrá ser completa, parcial o incompletamente accesible.

Para el caso de las características físicas, se considerarán como fuente principal de información aquella establecida en los datos de placa. Los criterios fundamentales a identificar en esta fase son los siguientes:

1. Capacidad total de almacenamiento de datos (típicamente expresada en GB).
2. Tipo de interfaz de conexión para alimentación y transferencia de información.
3. Datos del fabricante (modelo y/o versión del dispositivo).

Tal y como sucede con el caso de las características lógicas, cualquier perturbación que altere y/o impida la observación de estos parámetros también modificará la información que sea probable de ser obtenida a partir de una inspección visual de la carcasa del DDE estudiado (revisar estructura gramatical).

4.1.2 FASE 2: IDENTIFICACIÓN DEL TIPO DE FALLA PREDOMINANTE

Para esta sección, es necesario definir el principio fundamental bajo el cual el DDE analizado se encuentra sometido y, por lo tanto, imposibilitado de ser accedido por los métodos convencionales de operación.

Para el presente trabajo de investigación, se han presentado las definiciones para **daño lógico** y **daño físico** respectivamente, así pues, también se ha establecido que existen situaciones bajo las cuales una unidad de DDE puede experimentar un fallo de naturaleza lógica debido a la presencia de un fallo mecánico y viceversa. Sin embargo, ante un escenario de recuperación de información, es necesario definir la falla y causa principales, de esa forma y en función de estas, se podrá definir igualmente el conjunto de técnicas a implementar a fin de establecer los criterios de operación óptimos para ejecutar el proceso de recuperación de datos a partir del *software* desarrollado.

De forma general, en la tabla 46, se expresan el conjunto de consecuencias detectables y definidas para cada una de las fallas mecánicas y lógicas estudiadas, así como su naturaleza y principales causas características.

FALLAS MECÁNICAS	CAUSAS PRINCIPALES	CONSECUENCIAS DETECTABLES
ROTACIÓN NULA EN EL MOTOR DE EJE CENTRAL.	<ol style="list-style-type: none"> 1. Pérdida de las propiedades viscosas del fluido lubricante. 2. Fallo en el suministro eléctrico proporcionado por la 	<ol style="list-style-type: none"> 1. Incapacidad del equipo computacional para identificar la unidad y, por lo tanto, su contenido de

	<p>TCI.</p> <p>3. Deterioro y/o destrucción de los devanados internos por variaciones eléctricas.</p>	<p>información.</p> <p>2. Calentamiento en la TCI debido a la fricción producida por los electrones en los devanados.</p>
<p>SECTORES CON DAÑO FÍSICO.</p>	<p>1. Alteración manual del ambiente de operación e introducción de partículas y/o sustancias externas.</p> <p>2. Pérdida de la alineación paralela entre los soportes de los platos con respecto al cabezal.</p> <p>3. Degradación física en las cabezas de lectura y escritura.</p> <p>4. Fisuras en la superficie del plato magnetizable.</p>	<p>1. Dependiendo de la localización de los sectores: imposibilidad del sistema computacional para identificar la partición lógica.</p> <p>2. Destrucción de localidades y, con ello, de información.</p> <p>3. Aumento considerable en la ejecución de los tiempos de acceso en lectura y escritura de datos.</p> <p>4. Acceso restringido al volumen lógico parcial y/o total.</p>
<p>PATRÓN DE RAYADO EN EL PLATO MAGNETIZABLE.</p>	<p>1. Pérdida total de la posición de alineamiento</p>	<p>1. Destrucción total y definitiva de la información y el</p>

<p>PATRÓN DE RAYADO EN EL PLATO MAGNETIZABLE.</p>	<p>ortogonal entre la base del motor con respecto al actuador.</p> <ol style="list-style-type: none"> 2. Aplicación de impactos físicos antes y durante el estado de energización del DDE. 3. Expansión del material debido al sometimiento del DDE a la operación prolongada a altas temperaturas. 4. Súbitos cortes en la alimentación eléctrica y diferencias en el patrón de aire generado internamente en la carcasa. 	<p>medio físico donde reside, al igual que de los instrumentos implicados en el proceso de lectura y escritura.</p> <ol style="list-style-type: none"> 2. Aun energizado, no existe reconocimiento lógico del DDE.
<p>FALLAS LÓGICAS</p>	<p>CAUSAS PRINCIPALES</p>	<p>CONSECUENCIAS DETECTABLES</p>
<p>SECTORES CON DAÑO LÓGICO.</p>	<ol style="list-style-type: none"> 1. Presencia parcial o permanente de programas maliciosos tipo “virus informático”. 	<ol style="list-style-type: none"> 1. Aumento notorio en la ejecución de los tiempos de acceso en lectura y escritura de datos.

	<ol style="list-style-type: none"> 2. Corrupción del módulo <i>firmware</i>. 3. Bloqueo del sector por la influencia de un SO degradado. 4. Supresión súbita de la alimentación eléctrica al DDE. 5. Cualquier medio y forma de edición del micro-código interno aplicado al sector. 	<ol style="list-style-type: none"> 2. Dependiendo de la ubicación del sector dañado, puede prevenir la visualización de particiones y/o sus localidades y directorios.
<p>CORRUPCIÓN DE LA TABLA DE PARTICIONES.</p>	<ol style="list-style-type: none"> 1. Alteración manual y/o mediante <i>software</i>. 2. Borrado parcial y/o total del disco lógico. 3. Supresión súbita de la alimentación eléctrica al DDE. 4. Eliminación parcial y/o total de información debido a la presencia de virus informáticos. 	<ol style="list-style-type: none"> 1. Incapacidad del SO (nativo) para ser iniciado. 2. El <i>software</i> BIOS sólo detecta al DDE pero no así sus volúmenes lógicos. 3. Se le solicita al usuario la aplicación de un proceso de formateo (borrado de la información) a fin de restablecer el acceso a la partición. 4. La información del usuario es inaccesible por medios internos y externos.

<p>CORRUPCIÓN DE LA INFORMACIÓN DEBIDO A LA EJECUCIÓN DE <i>SOFTWARES</i> DEL TIPO “VIRUS INFORMÁTICO”.</p>	<ol style="list-style-type: none"> 1. Ausencia de un <i>software</i> de protección tipo “antivirus”, o bien, uno que se encuentre desactualizado. 2. Destrucción de las líneas de código que conforman los datos pertenecientes al AS y/o, principalmente, al AU. 3. Ejecución de un SO inestable debido a la alteración en su algoritmo de programación. 4. Complejidad en las dinámicas de operación del programa malicioso; esto previene al <i>software</i> antivirus de actuar y, por lo tanto, proteger al SO y los datos allí contenidos. 	<ol style="list-style-type: none"> 1. Eliminación parcial y/o total de los datos pertenecientes al AS y/o AU. 2. Restricción de acceso a la información del usuario. 3. Procesos de contagio masivos a través de la conexión física de dispositivos externos mediante interfaces tipo: USB (principalmente), SATA y/o IDE. 4. Alteración en las propiedades de manipulación y edición nativas a los archivos. 5. En ciertos casos, pérdida total del control operativo del sistema de cómputo infectado.
--	--	---

Tabla 46. Clasificación de las causas y consecuencias detectables en un DDE por influencia de las fallas mecánicas y lógicas expuestas.

Estos fenómenos (físicos y lógicos) son capaces de indicar ciertos síntomas, tanto en el disco lógico como en la unidad física, estos son cruciales para definir y clasificar el comportamiento del DDE y evaluar la aplicación de un proceso de recuperación de datos.

De forma general y de acuerdo a lo estudiado, en la tabla 46, se colocan la serie de comportamientos que una unidad de DDE puede experimentar cuando está sometida a un fallo lógico o mecánico persistentes.

TIPO DE FALLO	COMPORTAMIENTOS GENERALES DETECTADOS
1. LÓGICO.	<ol style="list-style-type: none"> 1. El DDE funciona mecánicamente pero no es reconocido por el <i>software</i> BIOS. 2. El identificador de la unidad (modelo) no se muestra visible dentro del apartado de unidades conectadas. 3. El identificador de la unidad (modelo) se muestra como visible, pero la capacidad de almacenamiento de la unidad no. 4. El SO instalado en la partición es ilegible. 5. Bajo ciertas circunstancias, se le solicita al usuario la aplicación de un proceso de formateo.
2. MECÁNICO.	<ol style="list-style-type: none"> 1. Para un fallo en el cabezal, se producen sonidos internos y/o golpeteos constantes; en adición, el DDE no es reconocido por el <i>software</i> BIOS. 2. Acceso nulo (ya sea que la unidad esté conectada como interna y/o externa). 3. Intermitencia de operación en el motor de eje central aun cuando existe alimentación eléctrica constante. 4. Visualización de la carbonización de elementos eléctricos y electrónicos pertenecientes a la TCI debido a la ausencia de medios de protección. 5. Aumento de temperatura en el dispositivo completo (carcasa, cubierta y TCI).

Tabla 47. Comportamientos generales característicos para las fallas mecánicas y lógicas pertenecientes a un DDE.

El *software* “FERCUVILL V5.0” sólo puede ser ejecutado y utilizado bajo la presencia de ciertas condiciones únicas de operación del DDE. Dichas condiciones de carácter indispensable/obligatorio, expresadas en la tabla 48, son las siguientes:

CONDICIONES FÍSICAS	CONDICIONES LÓGICAS
1. Funcionamiento (eléctrico-electrónico) total de la TCI y, en adición, del motor de eje central.	1. Reconocimiento pleno del DDE ante el <i>software</i> BIOS (incluido el modelo y capacidad total de almacenamiento de datos.
2. Integridad de los sectores físicos.	2. Desencadenamiento completo del micro-código asociado al sector RAP, de arranque y/o RISO.
3. Integridad de los elementos encargados de efectuar las maniobras de lectura y escritura de datos (TCI, circuito preamplificador, cable plano de datos, cabezas y platos magnetizables).	3. Existencia de una tabla de particiones en la que se especifiquen los tipos: primarias y secundarias y, en adición, que estas sean detectables como unidades lógicas accesibles.
4. Existencia de un equipo computacional “huésped”, tanto del DDE intervenido como del <i>software</i> mismo. En adición, la presencia de cables de conexión para datos y alimentación eléctrica.	4. Existencia de un SO compatible con la plataforma de operación. 5. Contemplar el espacio físico (unidad de DDE) y/o lógico (disco virtual) utilizado para efectuar la instalación del programa. 6. Contemplar el espacio físico y/o virtual correspondiente para efectuar el proceso de recuperación de información.

Tabla 48. Condiciones físicas y lógicas necesarias para utilizar el *software* “FERCUVILL V5.0” dentro de un marco de recuperación de información en unidades de DDE.

4.1.3 FASE 3: ANÁLISIS SOBRE LA VIABILIDAD DE LA UTILIZACIÓN DEL SOFTWARE “FERCUVILL V5.0”

En esta etapa se estudia (en función de los datos mostrados en las tablas 47 y 48) la posible aplicación del programa mencionado y los alcances de efectividad (relacionados a la capacidad de recuperación de información) reales que pueden ser obtenidos a partir de las condiciones físicas y lógicas existentes en el DDE afectado. El *software* desarrollado será aplicable sólo en ciertos casos específicos; así pues, debido al tipo de falla (lógica y/o mecánica) y de las condiciones predominantes de operación del DDE es que será: pertinente, conveniente y/o posible aplicar el método aquí expuesto.

De forma general y referida a las distintas fallas posibles y existentes en un DDE, El *software* “FERCUVILL V5.0” será esencialmente aplicable ante los siguientes escenarios de recuperación de datos:

1. Extracción de información en unidades de DDE degradadas en la estructura lógica del SO y/o *softwares* internos dependientes encargados de presentar la información a través de la ejecución del explorador de archivos.
2. Extracción de información en unidades de DDE degradadas en su estructura de AU y/o SO debido a la influencia y operación en estado permanente de *softwares* maliciosos tipo “virus informático” (el disco lógico debe de ser reconocido por el programa “*explorer.exe*”).
3. Extracción de información en unidades de almacenamiento de datos con un SA compatible con el algoritmo de programación del *software* propuesto, es decir, exclusivamente los tipos: NTFS y FAT32.
4. Recuperación efectiva del acceso a directorios y localidades internas de volúmenes lógicos bloqueados pertenecientes a un SO nativo y/o externo.
5. Restablecimiento lógico de la propiedad administrativa de objetos pertenecientes al usuario dentro de una partición lógica.
6. Restablecimiento de los valores virtuales iniciales de operación asociados a los programas nativos del SO.

7. Recuperación intensiva, extensiva y recursiva de información en dispositivos físicos (unidades de DDE) y volúmenes lógicos (particiones primarias y secundarias).

Para el caso planteado en el punto 2), la recuperación de la información está complementada por la ejecución, análisis y desinfección previa del DDE a partir de la utilización de un *software* del tipo “antivirus”.

El usuario podrá invocar y ejecutar el programa “FERCUVILL V5.0” si y sólo si el caso de recuperación de información se encuentra comprendido entre las capacidades y configuraciones expresadas previamente. No se debe de aplicar cuando los síntomas físicos y lógicos sean diferentes a los planteados, de lo contrario, se podría agravar el estado del DDE hasta un punto de deterioro tal en el que se ocasione una pérdida de datos masiva, irreparable y permanente.

4.1.4 FASE 4: UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0” (MÓDULOS ESPECÍFICOS)

Este apartado conforma el contenido medular del presente capítulo pues, debido a lo citado previamente, aquí se plantean, estudian, analizan y aplican los procedimientos y subrutinas del *software* “FERCUVILL V5.0” y sus módulos constitutivos a las diferentes muestras de unidades de DDE presentadas en el segundo capítulo del presente proyecto de investigación. De la misma forma y según corresponda, se aplican técnicas externas para completar el proceso de recuperación de información.

La ejecución del programa propuesto estará en función del tipo de daño presente y de las condiciones de operación de la unidad intervenida. Cada módulo desarrollado cuenta con una descripción concreta sobre las instrucciones y funciones que puede desempeñar y, a su vez, los resultados que pueden ser obtenidos.

Para esta etapa, se debe de contemplar y considerar al capítulo anterior como un eje de referencia mismo, pues, allí se describen y plantean los siguientes elementos:

1. Presentación y descripción detallada de los módulos estructurales del *software* desarrollado.

2. Ejecución y demostración del ambiente gráfico de operación y, en adición, los mensajes y comportamientos del SO asociado al programa.
3. Se colocan las funciones y los posibles escenarios de utilización dentro de un marco de recuperación de datos y/o de una extracción preventiva de información en unidades de DDE.
4. Requisitos de *hardware* y *software* necesarios para la instalación y ejecución del programa de forma permanente.

“FERCUVILL V5.0” puede invocar, de forma independiente, cada uno de sus módulos sin seguir un orden específico; sin embargo, se deben de respetar y seguir cada uno de los procesos de desinfección (por medio de un programa externo), limpieza, desbloqueo y, finalmente, extracción de datos para garantizar una recuperación de información consistente, efectiva y segura.

4.1.5 FASE 5: COMPROBACIÓN Y ANÁLISIS DE RESULTADOS

Esta constituye la etapa final del método expuesto para la recuperación de información. En la presente sección se evaluará el desempeño y funcionamiento del *software* expuesto en función de la cantidad y calidad de archivos restaurados y/o recuperados en cada una de las unidades físicas y lógicas intervenidas.

Debido a que cada tipo de archivo contiene, a su vez, un tipo único de extensión, la comprobación de resultados se realizará a partir de la apertura de cada uno de los objetos recuperados mediante los programas asociados a estos.

A su vez, el análisis de resultados se realizará mediante la comparación y comprobación de la unidad de DDE en sus diferentes estados: previo y posterior a la aplicación de “FERCUVILL V5.0” y/o, según corresponda, a la intervención física y/o lógica complementara al proceso de restauración de datos mismo.

4.2 APLICACIÓN DEL MÉTODO EN CASOS DE RECUPERACIÓN PROPUESTOS

En este apartado se analizarán y someterán los objetos de estudio planteados en la figura 31 y tablas: 25 y 28 a un proceso de recuperación de información formal a partir de la utilización del *software* “FERCUVILL V5.0”.

Las pruebas y procedimientos expuestos a continuación, como ya se ha planteado previamente, serán aplicados mediante la utilización de un sistema computacional y SO externos compatibles con el SA asociado a cada disco lógico de cada DDE intervenido; así como una plataforma virtual de operación que permita instalar y ejecutar de forma estable y permanente el *software* diseñado.

PROCESO DE RECUPERACIÓN Y EXTRACCIÓN DE INFORMACIÓN EN DISCO DUROS ELECTROMECAÑICOS

4.2.1 CASO DE RECUPERACIÓN 1

❖ FASE 1: PRESENTACIÓN DEL OBJETO ANALIZADO:

CARACTERÍSTICAS LÓGICAS IDENTIFICABLES:

1. Contiene una triada de particiones, de las cuales, la primera constituye la del tipo **primario**, en tanto que la segunda y tercera son del tipo **secundario**.
2. El DDE experimentó un daño consistente en la tabla de particiones secundaria (segunda partición), esta a su vez que fue reparada mediante la utilización de *software* semi-automatizado a través de una consola de recuperación externa.
3. Una vez restablecidas las entradas lógicas a cada una de las particiones, se realizó una comprobación de acceso a la unidad mediante la implementación del explorador de archivos (figura 34, ver página 78); se observó que la información del usuario se encontraba estratificada y organizada mediante directorios.
4. En la raíz principal de la unidad lógica recuperada, se visualizan un par de objetos ajenos al SO, usuario y/o *softwares* instalados en la partición primaria (“AUTORUN.EXE” y “autorun.inf”).

5. El acceso a la información, a través del explorador de archivos, es ineficaz. En adición, se observaron múltiples réplicas de los objetos extraños especificados en el punto anterior en distintas localidades del volumen.
6. Se determinó que la partición se encontraba deteriorada por la influencia de virus informáticos, en particular, por una variante modificada del tipo “ERS” en una etapa temprana. Se aplicó exitosamente un proceso de desinfección y eliminación forzada por medio de *software* tipo “antivirus”, con ello, se suprimieron todas aquellas réplicas, objetos y/o códigos maliciosos existentes.

CARACTERÍSTICAS MECÁNICAS IDENTIFICABLES:

1. En la tabla 20 y figura 32 (ver páginas: 79 y 80) se especifican y visualizan, respectivamente, los datos de placa y lógicos para la unidad de DDE descrita.
2. Esta unidad de DDE fue energizada eléctricamente para observar los comportamientos de los circuitos electrónicos y materiales conductores propios de la TCI; como resultado, se observó un pleno funcionamiento e identificación de la unidad ante el *software* BIOS del sistema computacional utilizado.
3. El motor de eje central no produjo sonidos y/o vibraciones que manifestaran un problema en los rodamientos.
4. **De acuerdo a los datos de placa proporcionados, este DDE cuenta con un certificado de reparación efectuado por la empresa desarrolladora de la unidad.**
5. Durante sus etapas de identificación, trabajo permanente y apagado, el DDE no mostró síntomas aparentes de deterioro en el cabezal, pues, no se identifican ruidos y/o sonidos extraños internos a la carcasa.

Pese a la supresión en la fuente de alimentación eléctrica y el daño lógico producido en la tabla de particiones, esta unidad se encuentra en condiciones mecánicas y virtuales óptimas para ser sometida al método expuesto.

❖ FASE 2: IDENTIFICACIÓN DEL TIPO DE FALLA PREDOMINANTE:

Para el caso particular de este DDE, el tipo de daño es **lógico debido a una condición dinámica** producido por el corte súbito del suministro eléctrico durante la aplicación de un

proceso virtual que implicaba la manipulación directa por *software* (expansión del tamaño del volumen) de la tabla de particiones.

Si bien la reconstrucción del acceso a la tabla de particiones fue exitosa, cuando el sector RAP es perturbado física y/o lógicamente es imperativo ejecutar inmediatamente un proceso extracción de información, pues, de dicha estructura depende por completo el acceso a todo el contenido virtual del DDE.

❖ **FASE 3: ANÁLISIS SOBRE LA VIABILIDAD DE LA UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0”:**

Posterior al proceso lógico de reparación aplicado al DDE en su tabla de particiones, este cumple y satisface las condiciones descritas en la tabla 48 del presente proyecto de investigación, por lo tanto, se establece que este dispositivo es candidato para que se le aplique el método de recuperación de información propuesto mediante la intervención lógica del *software* “FERCUVILL V5.0”.

• **FASE 4: UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0” (MÓDULOS ESPECÍFICOS):**

El disco lógico fue desinfectado exitosamente, tanto del código base (“autorun.inf”) como de las distintas réplicas ejecutables (“AUTORUN.EXE”). Como consecuencia directa, el directorio principal se visualiza de la siguiente forma (figura 108).

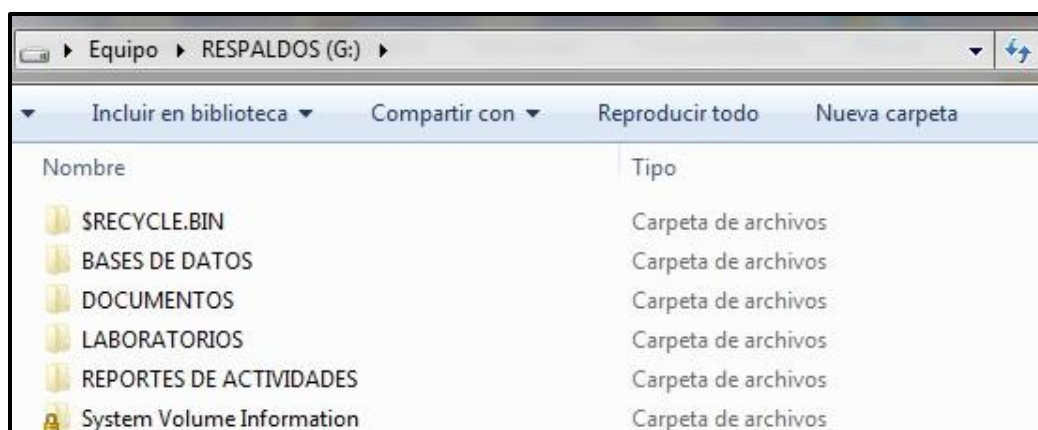


Figura 108. Visualización del contenido del volumen lógico “G:” posterior al proceso de desinfección.

La información no puede ser editada debido a que, pese a que ya no existe influencia permanente de código malicioso, los estragos relacionados al deterioro de las propiedades de las carpetas y archivos aún son persistentes.

APLICACIÓN DEL MÓDULO 7: H. A. A. B.

Por su descripción, este *software* constitutivo será el encargado de restaurar el acceso a la información del volumen a partir de la intervención de sus propiedades lógicas comprendidas dentro del SO (figura 109).

1. Ejecutar la ventana principal de operación del MÓDULO 7: H. A. A. B.

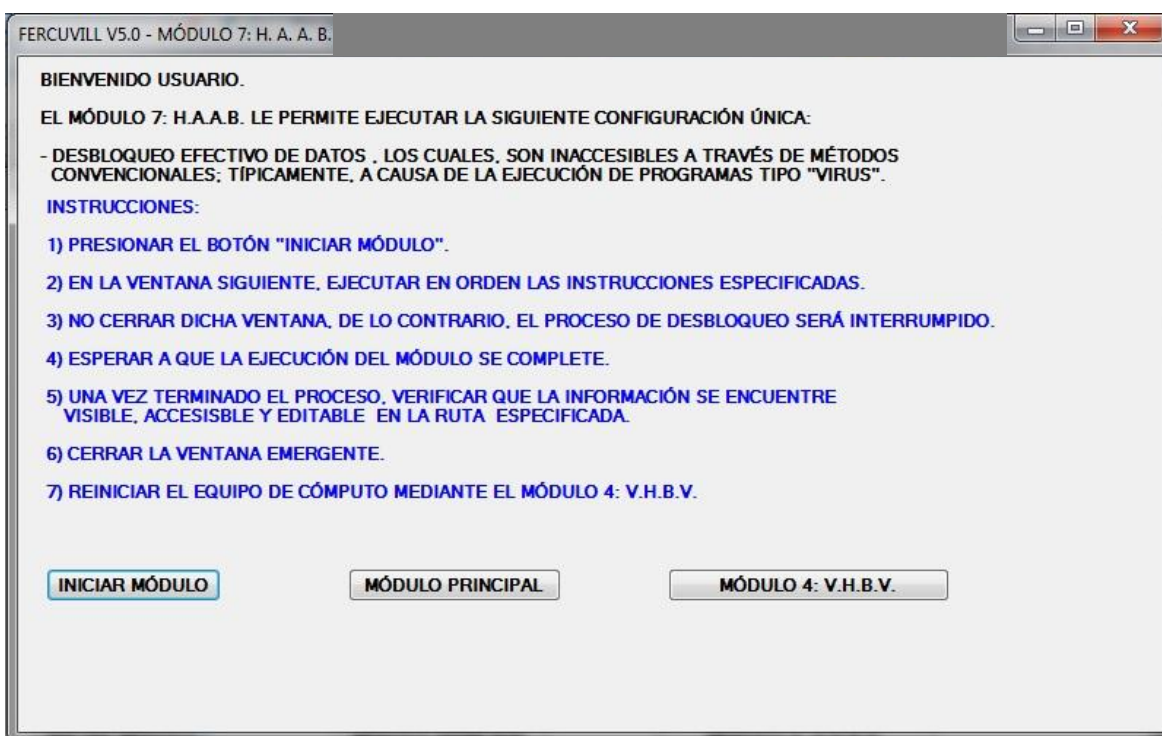


Figura 109. Ventana principal de operación del MÓDULO 7: H. A. A. B.

CONSIDERACIONES PREVIAS A LA EJECUCIÓN DEL MÓDULO:

1. El disco lógico “G:” fue aislado de ser utilizado por otras aplicaciones en primer y segundo plano.
2. Para evitar problemas de compatibilidad y de lectura de zonas específicas del volumen intervenido, la protección por *software* “antivirus” fue desactivada de forma parcial.

3. Todas las aplicaciones relacionadas a las extensiones de los archivos contenidos en la partición deben de ser cerradas.
2. **Iniciar el módulo base e invocar la consola tipo MS-DOS presentada como ventana emergente (figura 110).**



Figura 110. Consola principal de operación en ambiente MS-DOS del MÓDULO 7: H. A. A. B.

3. **Selección del argumento "G:" como dispositivo para ser intervenido (figura 111).**

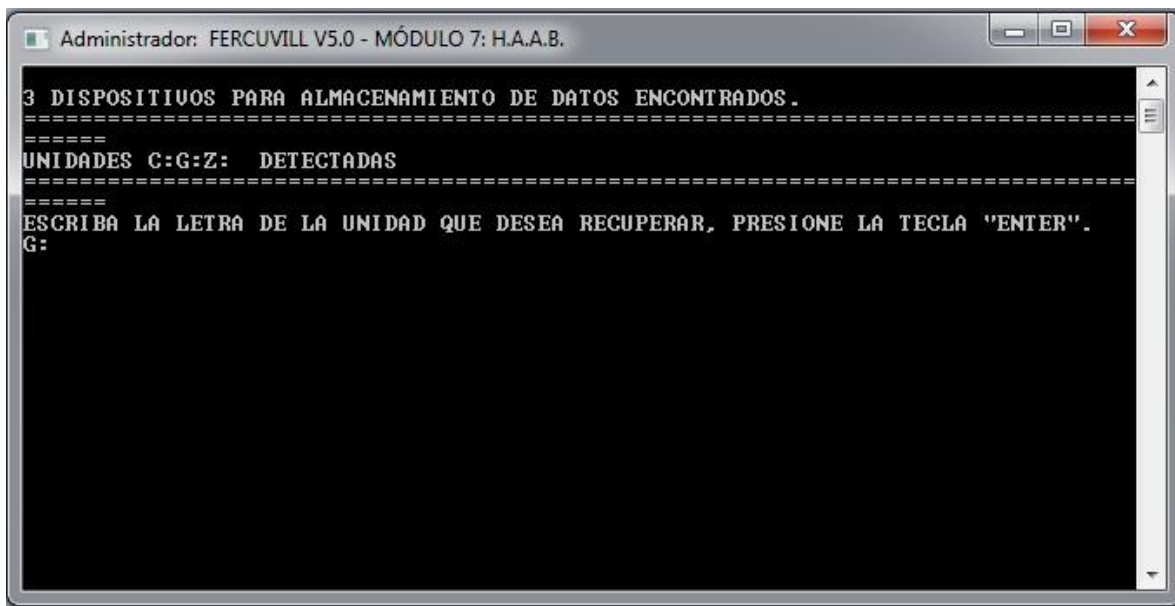


Figura 111. Selección de la unidad lógica descrita por el argumento "G:" como aquella a ser modificada por la consola externa.

Posterior a los mensajes del sistema (figuras: 98, 99, 100, 101, 104, 105 y 106), la consola indicará el término de su ejecución y reportará los resultados obtenidos (figura 112).

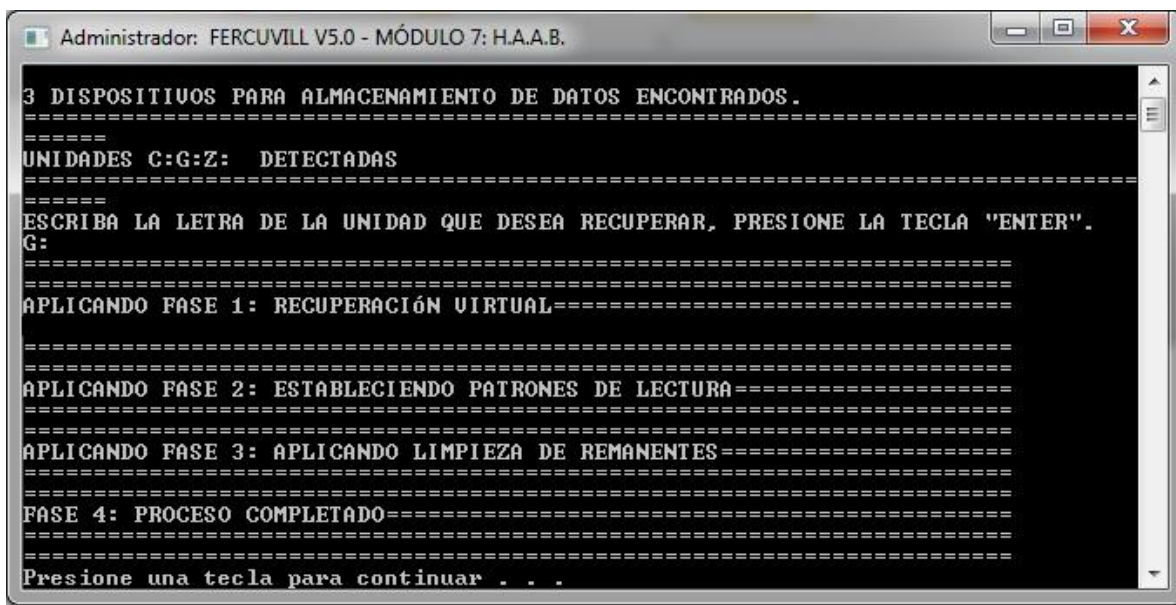


Figura 112. Ejecución de las etapas de desbloqueo de información sobre el objeto especificado como “G:” mediante la utilización de la consola externa.

Una vez aplicado este módulo, se procede a verificar los cambios realizados a los directorios y sus contenidos (figura 113) mediante la utilización del explorador de archivos.

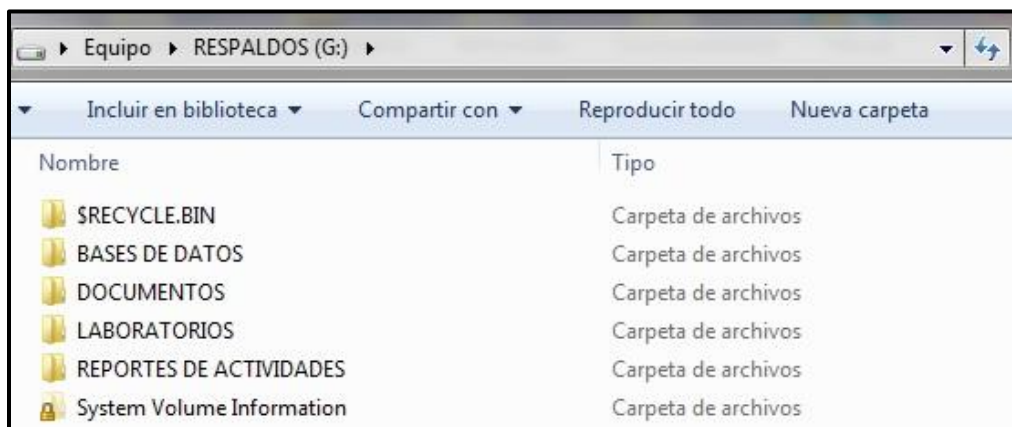


Figura 113. Visualización del volumen lógico “G:” a través del *software* “*explorer.exe*” para una intervención exitosa del MÓDULO 7: H. A. A. B.

Los directorios pertenecientes al usuario se encuentran desbloqueados y editables, sin embargo y puesto que ya se ha aplicado una restauración lógica preliminar (reparación de la tabla de particiones), es imperativo aplicar un proceso de extracción de datos inmediato, para este escenario en particular, se utilizará el MÓDULO 2: S. V. B.

APLICACIÓN EL MÓDULO 2: S. V. B.

Por su descripción, este *software* primario es el encargado de proporcionar una interfaz gráfica de operación para efectuar procedimientos de extracción de datos bajo un ambiente operacional dentro de un SO.

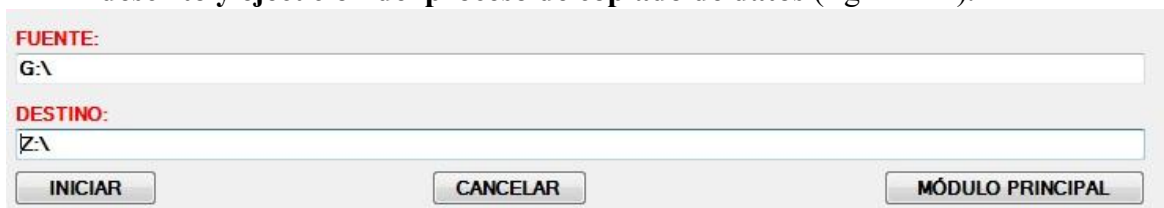
1. Ejecutar la ventana principal de operación del **MÓDULO 2: S. V. B.** (figura 63)
2. Establecer los parámetros de “FUENTE” y “DESTINO” propios para cada caso.

Para este escenario de recuperación de datos, se utilizó una unidad de DDE “destino” cuyos datos de placa (y lógicos) son presentados a continuación en la tabla 49.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	SEAGATE.
MODELO.	ST3320413CS.
DBL.	625142448 SECTORES.
INTERFAZ.	SATA.
CAPACIDAD DE ALMACENAMIENTO.	320 GB.
DATOS LÓGICOS	DESCRIPCIÓN
VOLÚMENES CONTENIDOS.	1 DISCO LÓGICO (UNIDAD “Z:”).

Tabla 49. Datos de placa y lógicos para DDE “DESTINO” utilizado en el proceso de extracción de información mediante el MÓDULO 2: S. V. B.

3. Establecimiento de los parámetros de operación en el *software* primario descrito y ejecución del proceso de copiado de datos (figura 114).



The screenshot shows a configuration window with two input fields. The first field is labeled 'FUENTE:' and contains the text 'G:\'. The second field is labeled 'DESTINO:' and contains the text 'Z:\'. Below the input fields are three buttons: 'INICIAR', 'CANCELAR', and 'MÓDULO PRINCIPAL'.

Figura 114. Establecimiento de los parámetros “FUENTE” y “DESTINO” dentro del MÓDULO 2: S. V. B.

4. Inicio del proceso de recuperación de información.

Los directorios contenidos en el volumen lógico fueron extraídos de forma correcta. Existen ciertas piezas de información tales como *softwares* cuyo tamaño es considerable y, para este caso, uno de estos fue detectado e igualmente recuperado; este elemento se utiliza de referencia para poder observar el ambiente de barra de progreso y velocidades variables de lectura y escritura de datos presentes durante el proceso descrito (figura 115).

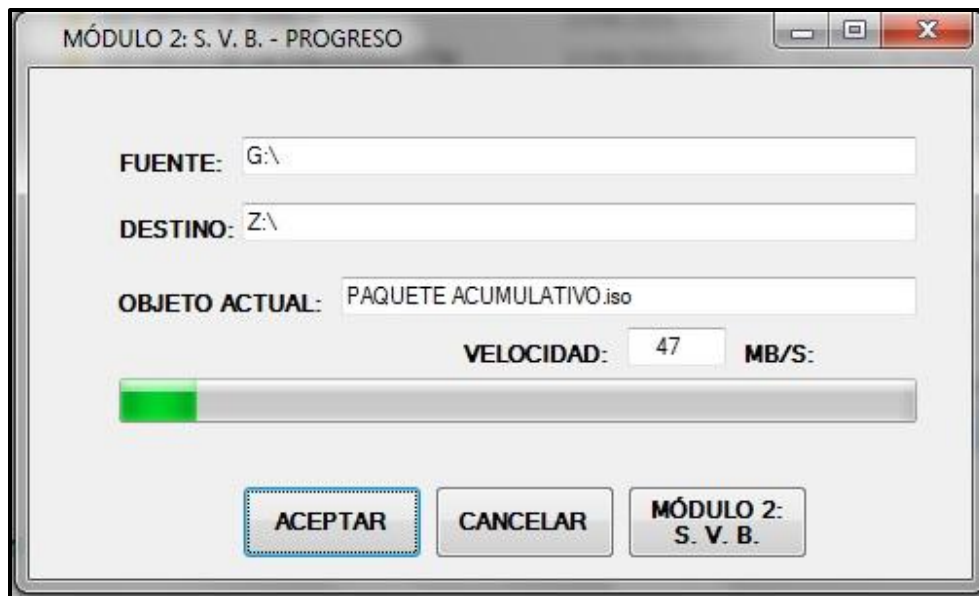


Figura 115. Ventana de progreso para un proceso de extracción de datos iniciado por el MÓDULO 2: S. V. B.

Una vez finalizado el procedimiento, mediante la utilización del explorador de archivos, se procedió a corroborar que la información deseada a ser recuperada en efecto se encontraba en la ubicación “DESTINO”; esta condición fue comprobada completamente y, por lo tanto, **la recuperación de información ha sido lograda en esta unidad de DDE.**

- **FASE 5: COMPROBACIÓN Y ANÁLISIS DE RESULTADOS:**

La información fue ejecutada por medio de la utilización de los *softwares* asociados a las extensiones mismas de los archivos, así mismo, estos se encontraban sin corromper y con el avance (modificaciones realizadas por el usuario) desarrollado previo al fallo lógico de la tabla de particiones y recuperación virtual posterior ejecutada por el programa “FERCUVILL V5.0”.

Las extensiones identificadas en esta unidad son las siguientes: “.doc”, “.docx”, “.accdb”, “.xls”, “.xlsx”, “.iso” y “.pptx”.

4.2.2 CASO DE RECUPERACIÓN 2

- **FASE 1: PRESENTACIÓN DEL OBJETO DE ESTUDIO ANALIZADO:**

CARACTERÍSTICAS LÓGICAS IDENTIFICABLES:

1. El disco lógico “F:” constituye la partición única y, por lo tanto, del tipo **primario** asociada al DDE modelo: “5T020H2” (tabla 25) que contiene la información del SO y del usuario.
2. El volumen lógico es detectado y leído exitosamente por los *softwares*: BIOS, “*explorer.exe*” y “*diskmgmt.msc*”.
3. Se aplicó un procedimiento de desinfección y eliminación forzada de amenazas correspondientes a *softwares* tipo “virus”, específicamente, del tipo “troyano”.
4. El SO nativo del DDE se encuentra degradado en sus estructuras virtuales, sin embargo y mediante la utilización de herramientas de diagnóstico externas, se determinó que los daños aplicados por los programas víricos no han afectado las localidades asociadas a la información del usuario.
5. Debido a las acciones del *software* “troyano”, los permisos administrativos de acceso y posesión de datos, al igual que las características de lectura; se encuentran deshabilitados. Por esta misma circunstancia, la información puede ser extraída siempre y cuando el SO utilizado obtenga la propiedad de dichos directorios.

CARACTERÍSTICAS MECÁNICAS IDENTIFICABLES:

1. A continuación, en la tabla 50, se especifican los datos de placa (y lógicos) para la unidad de DDE descrita.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	MAXTOR.
MODELO.	5T020H2.
DBL.	39062500 SECTORES.
INTERFAZ.	IDE.
CAPACIDAD DE ALMACENAMIENTO.	20 GB.
DATOS LÓGICOS	DESCRIPCIÓN
VOLÚMENES CONTENIDOS.	2 VOLÚMENES (UNIDADES “F:”,”W:”).

Tabla 50. Datos de placa y lógicos para un DDE deteriorado en su volumen principal por causa de amenazas tipo “troyano”.

2. Esta unidad de DDE fue energizada eléctricamente para observar los comportamientos de los circuitos electrónicos y materiales conductores propios de la TCI; como resultado, se observó un pleno funcionamiento e identificación de la unidad ante el *software* BIOS del sistema computacional utilizado.
3. El motor de eje central no produjo sonidos y/o vibraciones que manifestaran un problema con los rodamientos.
4. La unidad de DDE presentó un calentamiento generalizado cuando se le mantuvo en funcionamiento y ejecutando los procesos de desinfección. Este factor es significativo pues, de “demandar” en mayor proporción recursos de *hardware* y *software*, las características de operación estable de la unidad podrían perderse y el DDE averiarse por contacto físico entre la cabeza y el plato magnetizable debido a la expansión del material constitutivo.
5. El proceso de lectura de datos (mediante el explorador de archivos) resultó ser el que exigió de mayor forma a la unidad de DDE, la razón posible de esto es un

deterioro en los instrumentos asociados a la inserción y extracción de señales magnéticas desde y hacia los platos magnetizables. Bajo la condición previamente descrita, es necesario recuperar inmediatamente la información alojada en esta unidad pues, de forma inadvertida (la tecnología S.M.A.R.T. no pudo ser obtenida en este DDE), esta podría dejar de funcionar y la pérdida de información sería inminente.

El proceso de extracción de datos es realizado en una sola exhibición mediante la utilización de una unidad de DDE acoplada a través de sus interfaces de conexión nativas hacia el sistema computacional principal que, a su vez, también contiene al DDE estudiado.

- **FASE 2: IDENTIFICACIÓN DEL TIPO DE FALLA PREDOMINANTE:**

Este dispositivo se encuentra funcionando inestablemente en condiciones físicas y lógicas en deterioro progresivo. Si bien no se ha manifestado un tipo de falla (pues se han aplicado apropiadamente técnicas de *software* y *hardware*) en particular, esta puede surgir y presentarse como **una de tipo mecánico por una condición lógica** (debido al calentamiento previamente mencionado y/o a la antigüedad del dispositivo mismo y su desgaste consecuente) y viceversa (fallo lógico en los sectores de los platos debido a la avería en los circuitos físicos de la TCI).

- **FASE 3: ANÁLISIS SOBRE LA VIABILIDAD DE LA UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0”:**

Se determinó, posterior a la evaluación de las condiciones lógicas y mecánicas de la unidad estudiada, que este DDE es candidato para que se le aplique el método de recuperación de información propuesto mediante la intervención lógica del *software* “FERCUVILL V5.0”.

- **FASE 4: UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0” (MÓDULOS ESPECÍFICOS):**

La desinfección aplicada a la partición fue completada y comprobada exitosamente; sin embargo y puesto que este volumen fue deteriorado en diferentes estructuras, es necesario aplicar un proceso de extracción de datos orientado y específico. Este proceso consiste en la

identificación de las localidades (directorios) en las que exista, exclusivamente, información producida por el usuario y/o *softwares* manipulados por este.

Se realizó un estudio y exploración de la unidad citada y, como resultado, se observó que las siguientes ubicaciones contienen datos y extensiones relacionadas relevantes para el presente método expuesto:

- La ruta “**F:\Documents and Settings**”, que contiene automáticamente los directorios: “Mis Documentos”, “Mis Imágenes”, “Mis Videos”, “Mi Música”, pero también resguarda otros editados y creados por el usuario (figura 116).

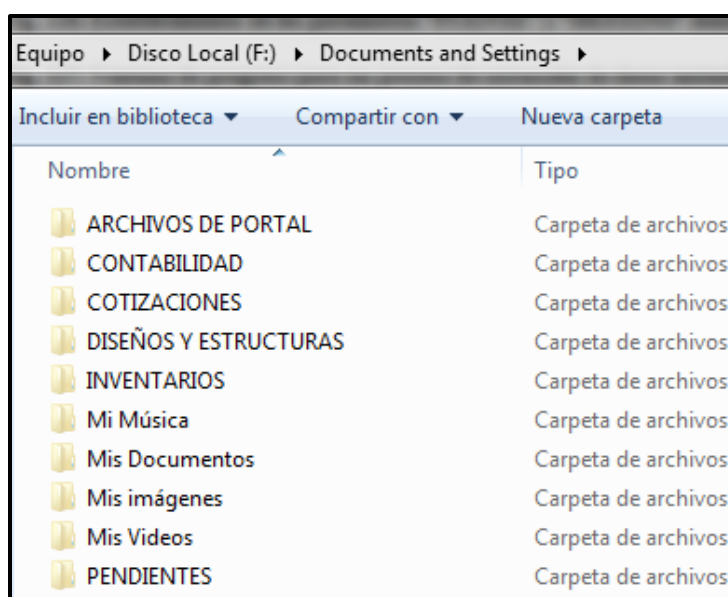


Figura 116. Visualización del directorio principal contenedor de información del usuario en el volumen “F:” posterior al proceso de desinfección y eliminación forzada de *software* malicioso.

La información no puede ser editada debido a que, por acción directa ejecutada por las amenazas tipo “troyano”, el volumen ha perdido sus propiedades administrativas (aquellas que le permiten al SO tomar posesión y propiedad del contenido de directorios) y de lectura (el acceso es restringido y la información no permite ser manipulada).

Durante las etapas de análisis y estudio previos a la aplicación del *software* desarrollado, se corroboró que este disco lógico cuenta con una cantidad de información posible a recuperar aproximadamente igual a 13.84 GB. El valor anterior tiene especial relevancia puesto que se deben de contemplar las siguientes condiciones antes de ejecutar el proceso de recuperación de información:

1. Exponer al DDE a una operación constante y prolongada podría ocasionar una avería física y/o lógica permanente, destruyéndose así la información contenida en el dispositivo, por ello, la extracción de datos debe de realizarse de forma localizada.
2. Los directorios de mayor tamaño deben de ser extraídos primero, de esa forma, el DDE sufrirá un menor estrés mecánico al enfocarse en sectores (mayoritariamente) consecutivos entre sí.
3. Los procedimientos de desbloqueo y recuperación de las propiedades administrativas deben de realizarse de forma previa a la recuperación de las propiedades de lectura de datos.

APLICANDO EL MÓDULO 7: H. A. A. B.

Por su descripción, este *software* constitutivo será el encargado de restaurar el acceso a la información del volumen a partir de la intervención de sus propiedades lógicas comprendidas dentro del SO (figura 117).

1. Ejecutar la ventana principal de operación del MÓDULO 7: H. A. A. B.

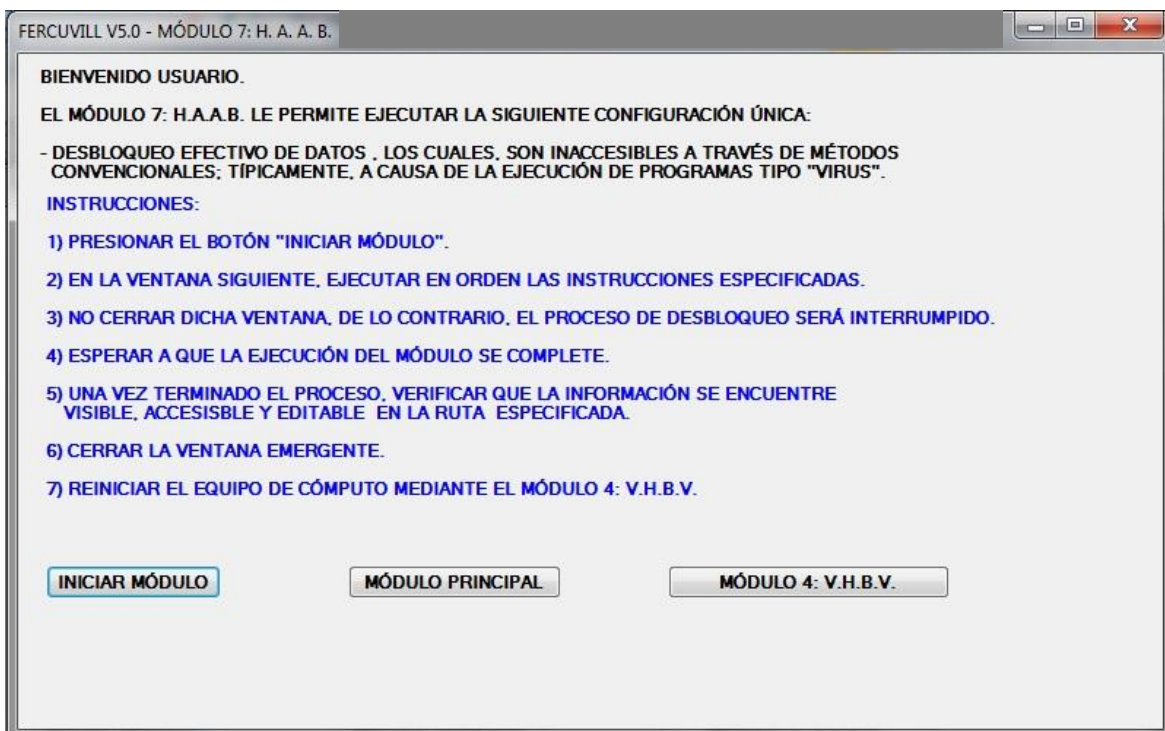


Figura 117. Ventana de principal de operación del MÓDULO 7: H. A. A. B.

CONSIDERACIONES PREVIAS A LA EJECUCIÓN DEL MÓDULO:

1. El disco lógico “F:” fue aislado de ser utilizado por otras aplicaciones en primer y segundo plano.
 2. Para evitar problemas de compatibilidad y de lectura de zonas específicas del volumen intervenido, la protección por *software* “antivirus” fue desactivada de forma parcial.
 3. Todas las aplicaciones relacionadas a las extensiones de los archivos contenidos en la partición deben de ser cerradas.
 4. La consola externa de operación en ambiente MS-DOS únicamente detectará a la unidad afectada descrita “F:” y al volumen lógico principal del sistema computacional utilizado para la ejecución de “FERCUVILL V5.0”, es decir, “C:”. la conexión del DDE empleado para resguardar la información será posterior a las modificaciones aplicadas por el MÓDULO 7: H. A. A. B.
- 2. Inicio del módulo base y apertura de la consola en ambiente MS-DOS presentada como ventana emergente (figura 118).**

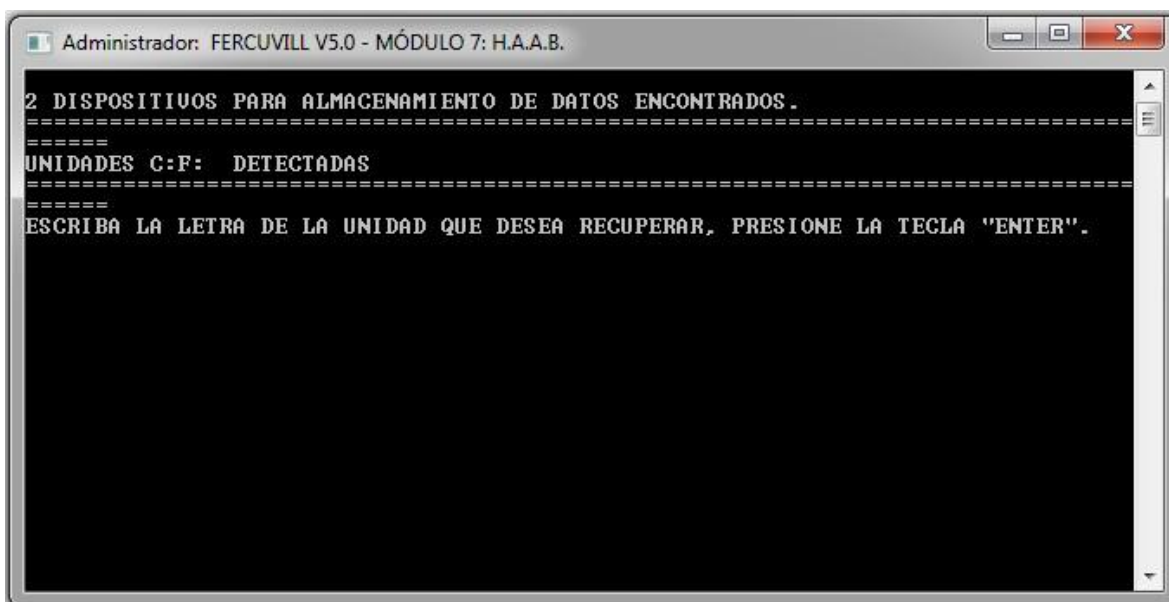


Figura 118. Consola externa de operación en ambiente MS-DOS del MÓDULO 7: H. A. A. B.

CONSIDERACIONES DURANTE ESTA ETAPA:

1. Si el acceso a la unidad (figura 120) supera un periodo de tiempo máximo igual a 2 minutos, el MÓDULO 7: H. A. A. B. debe de ser cerrado manualmente, el equipo

computacional reiniciado y, posterior a este último, “FERCUVILL V5.0” deberá ser ejecutado nuevamente.

2. El proceso, una vez iniciado, no deberá de ser interrumpido de forma directa (intervención del usuario) y/o indirecta (bloqueo o intervención de otro *software*).
3. **Selección del argumento “F:” como aquel dispositivo a ser intervenido** (figura 119).

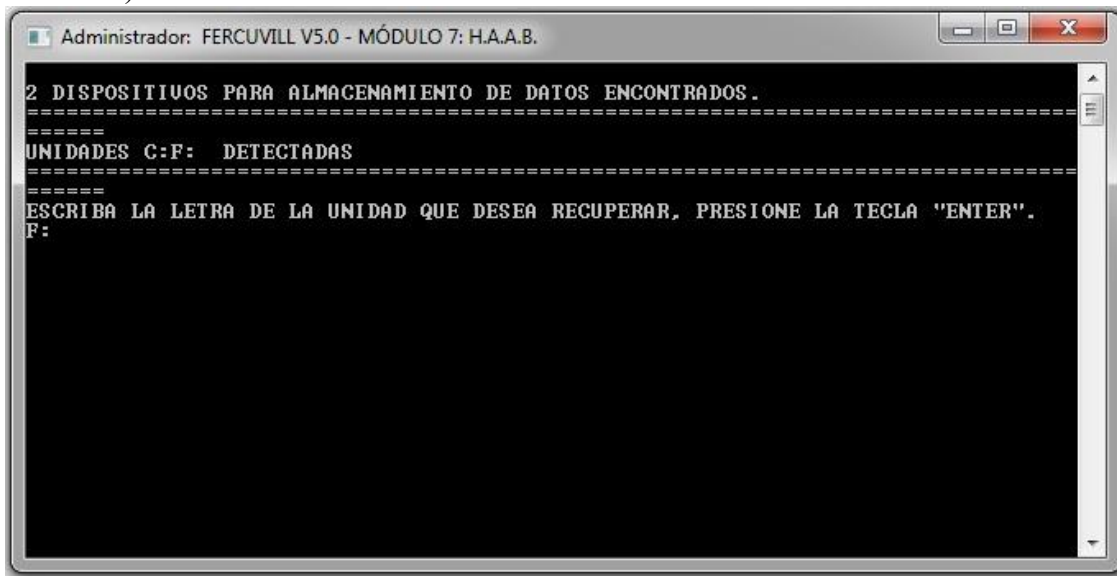


Figura 119. Selección de la unidad lógica descrita por el argumento “F:” como aquella a ser modificada por la consola externa.

Posterior a los mensajes del sistema (figuras: 98, 99, 100, 101, 104, 105 y 106), la consola indicará el término de su ejecución y reportará los resultados obtenidos (figura 120).

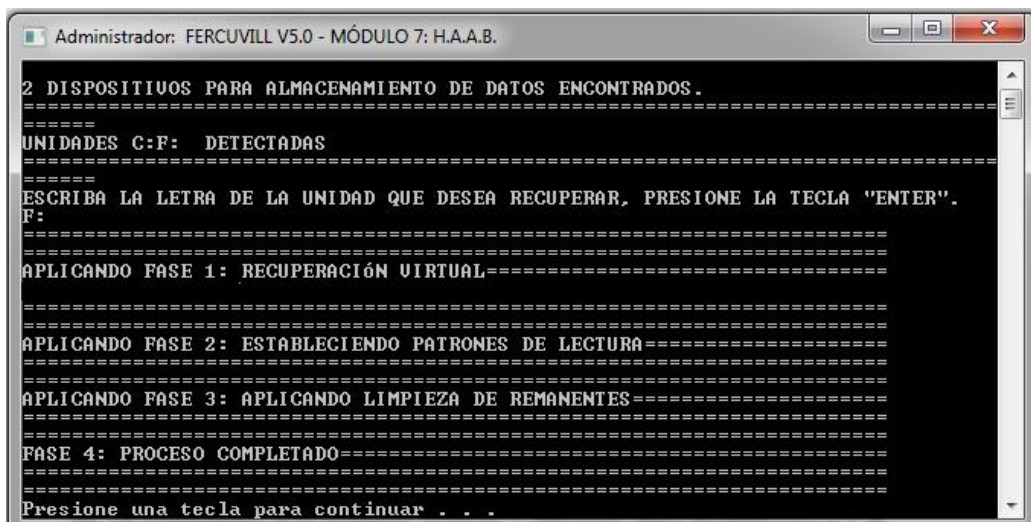


Figura 120. Ejecución de las etapas de desbloqueo sobre el objeto especificado como “F:” mediante la utilización de la consola externa.

Una vez aplicados los procesos de este módulo, se procede a verificar los cambios efectuados a los directorios y sus contenidos mediante la utilización del explorador de archivos (figura 121).

La información se encuentra nuevamente disponible en la unidad, sin embargo y a diferencia del caso de recuperación anteriormente expuesto, no existen permisos por parte del SO “huésped” del DDE para acceder y editar los directorios.



Figura 121. Visualización del volumen lógico “F:” a través del *software* “explorer.exe” para una intervención completa del MÓDULO 7: H. A. A. B.

Como ya se mencionó anteriormente, el intento de acceder a cualquier localidad del volumen “F:” tiene como resultado el siguiente mensaje en pantalla (figura 122):



Figura 122. Visualización de error en pantalla por acceso fallido debido a la usencia de permisos administrativos en el volumen “F:”.

APLICANDO MÓDULO 5: P. A. H.

De acuerdo a su descripción, este *software* ejecutará el algoritmo que permita conceder acceso a la información existente en el volumen intervenido.

1. Ejecución de la ventana principal de operación del MÓDULO 5: P. A. H. (figura 123).

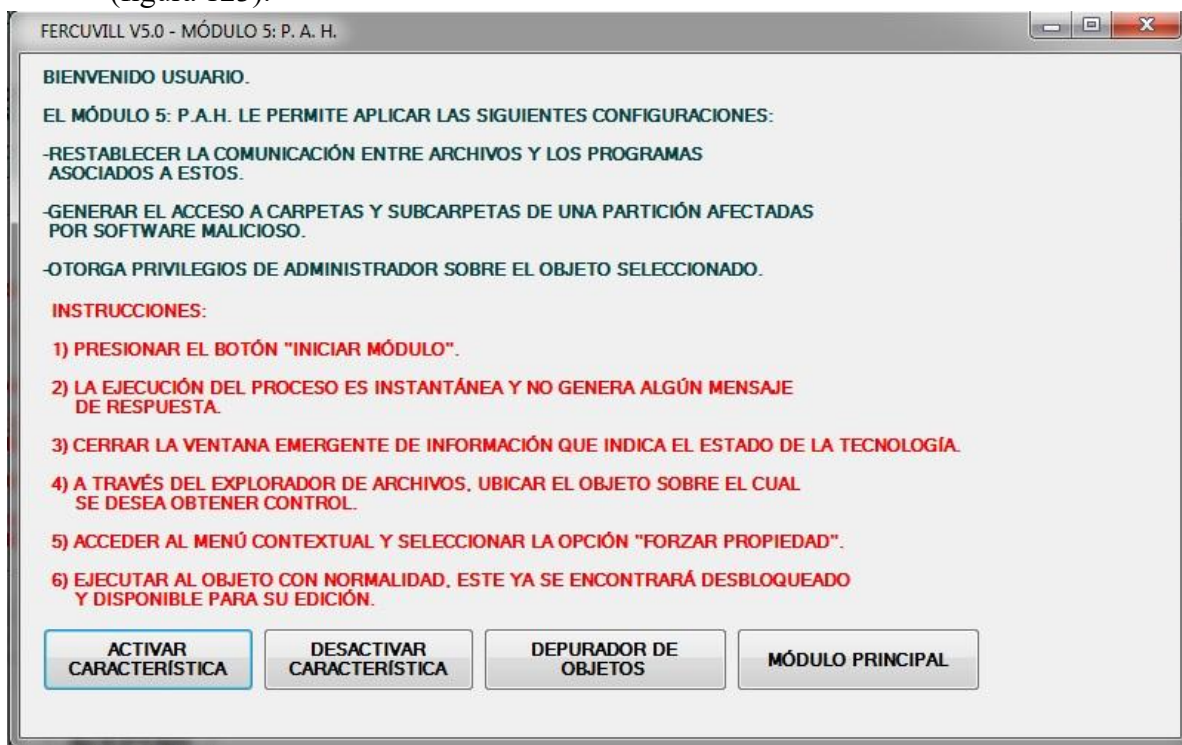


Figura 123. Interfaz gráfica de operación para el MÓDULO 5: P. A. H.; visualización de “INSTRUCCIONES”, y “BOTONES DE CONTROL”.

2. Seleccionar la opción identificada como “ACTIVAR CARACTERÍSTICA”.
3. Presionar el botón “Aceptar” localizado en la ventana emergente (ver figura 90).

4. Seleccionar, con el botón secundario, cada uno de los directorios internos del volumen asociado al DDE estudiado e identificar (en el menú contextual) la opción llamada “FORZAR PROPIEDAD”, presionarla (figura 124).

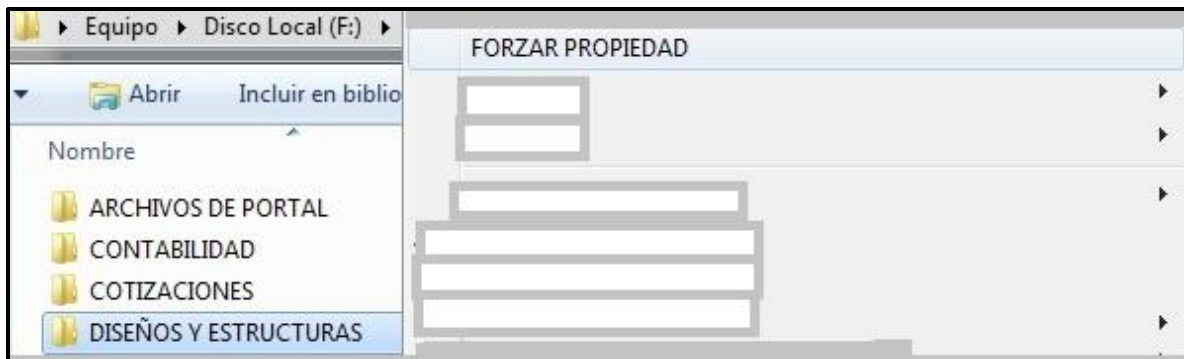


Figura 124. Selección de la característica “FORZAR PROPIEDAD” en un directorio específico para un restablecimiento de las propiedades administrativas de un objeto particular.

Considerando como referencia la localidad llamada “INVENTARIOS”, se procedió a comprobar si su contenido estaba visible y editable y, de hecho, este se encontraba ya disponible para su edición y extracción hacia una unidad externa (figura 125).

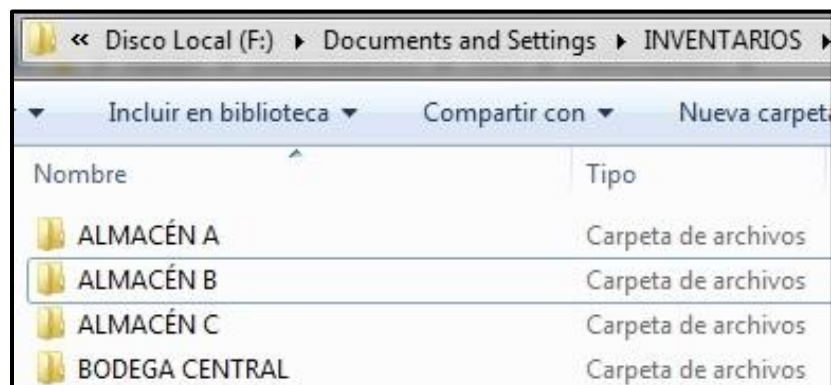


Figura 125. Visualización de un disco lógico posterior a la aplicación del MÓDULO 5: P. A. H. para la obtención de propiedades administrativas en un directorio particular.

5. Ejecutar un reinicio del sistema computacional mediante la utilización del MÓDULO 4: V. H. B. V., en el apartado “ASISTENTE AVANZADO DE INICIO”, en la opción “REINICIO” y, finalmente, en “PROCEDER”. De esa forma, los cambios efectuados serán de carácter permanente (figuras: 77 y 79 ver páginas 177 y 178, respectivamente).

El disco lógico “F:” constituye el volumen primario principal del DDE analizado, sin embargo y por las condiciones lógicas establecidas en las tablas 25 y 26, este dispositivo aún se encuentra experimentando una infección a causa de una variante modificada de “virus polifórmico”, si bien esta no pertenece al volumen estudiado en esta sección, siempre existe un riesgo latente en el que la información extraída se encuentre infectada.

Atendiendo al planteamiento anterior, se ejecutará el MÓDULO 6: S. H. B. V. como un procedimiento alternativo y preventivo ante un escenario de infección entre volúmenes.

APLICACIÓN DEL MÓDULO 6: S. H. B. V.

De acuerdo a sus características de funcionamiento, este *software* prevendrá a cualquier módulo de copiado de extraer objetos cuyas características no sean compatibles con su base de datos interna, si y sólo si, la unidad de “destino” para dicho proceso de extracción contiene una interfaz tipo USB.

1. Ejecución de la ventana principal de operación del MÓDULO 6: S. H. B. V. (figura 126).

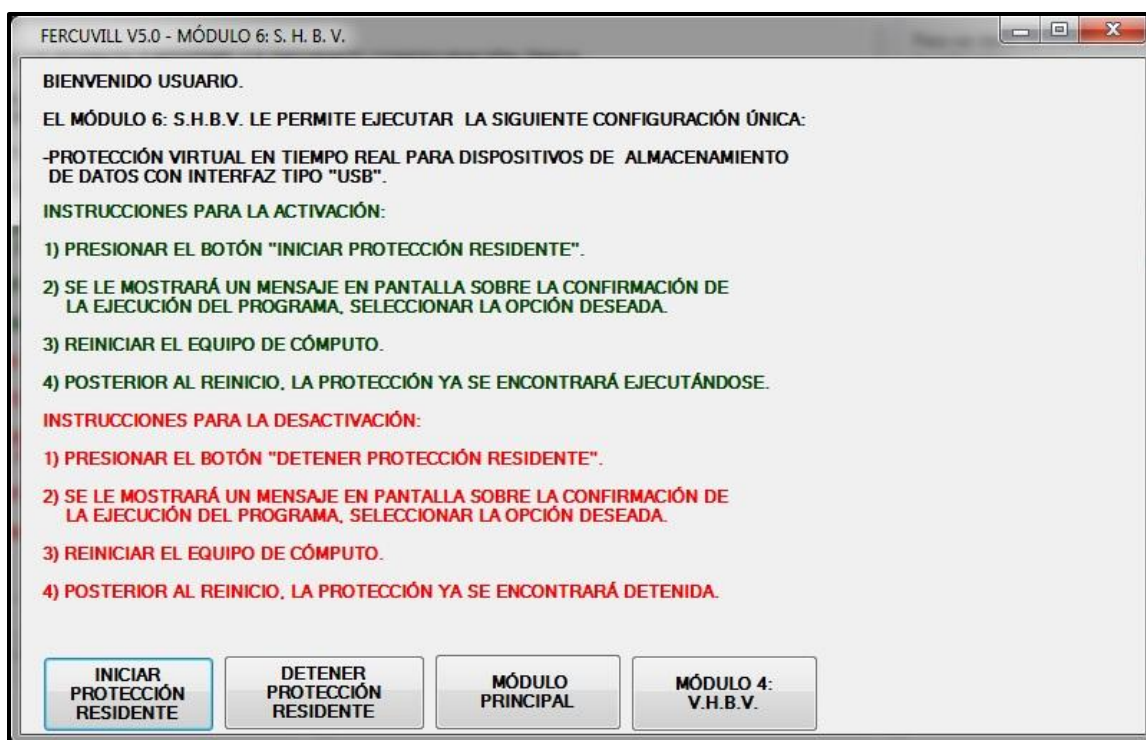


Figura 126. Interfaz gráfica de operación para el MÓDULO 6: S. H. B. V.

2. **Seleccionar y presionar la opción identificada como “INICIAR PROTECCIÓN RESIDENTE”.**
3. **De acuerdo a lo indicado por la ventana emergente (figura 127), proceder a aplicar la característica y esperar a que el proceso sea completado.**

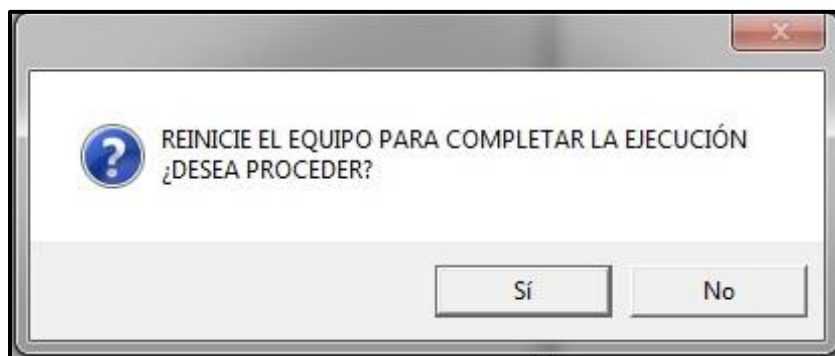


Figura 127. Mensaje del sistema (19): solicitud de continuación y reinicio del sistema.

4. **Ejecutar un reinicio del sistema computacional mediante la utilización del MÓDULO 4: V. H. B. V., en el apartado “ASISTENTE AVANZADO DE INICIO”, en la opción “REINICIO” y, finalmente, en “PROCEDER”. De esa forma, los cambios efectuados serán de carácter permanente (figuras: 78 y 80, ver páginas 173 y 174, respectivamente).**

Una vez establecidas las propiedades de cada uno de los objetos pertenecientes al volumen principal y sus respectivas tecnologías de protección, se procede a aplicar el proceso de extracción de datos a partir de la utilización del MÓDULO 2: S. V. B.

APLICACIÓN DEL MÓDULO 2: S. V. B.

De acuerdo a su descripción, este *software* permite establecer rutas (tanto para el “origen” como la “fuente” de información) personalizadas para invocar el proceso de recuperación de datos.

1. **Ejecutar la ventana principal de operación del MÓDULO 2: S. V. B. (figura 63).**
2. **Establecer los parámetros de “FUENTE” y “DESTINO” propios para cada caso.**

Para este escenario de recuperación de datos, se utilizó una unidad de DDE “destino” cuyos datos de placa (y lógicos) son presentados a continuación en la tabla 51.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	WESTERN DIGITAL.
MODELO.	WDBACX0010BBK-NESN
DBL.	1953525168 SECTORES.
INTERFAZ.	USB.
CAPACIDAD DE ALMACENAMIENTO.	1000 GB.
DATOS LÓGICOS	DESCRIPCIÓN
VOLÚMENES CONTENIDOS.	1 DISCO LÓGICO (UNIDAD “R:”).

Tabla 51. Datos de placa y lógicos para DDE “DESTINO” utilizado en el proceso de extracción de información mediante el MÓDULO 2: S. V. B.

3. Establecimiento de los parámetros de operación específicos en el *software* primario descrito y ejecución del proceso de copiado de datos (figura 128).

The image shows a software window with two input fields. The first field, labeled 'FUENTE:', contains the text 'F:\Documents and Settings'. The second field, labeled 'DESTINO:', contains the text 'R:\'. Below these fields are three buttons: 'INICIAR', 'CANCELAR', and 'MÓDULO PRINCIPAL'.

Figura 128. Establecimiento de los parámetros “FUENTE” y “DESTINO” dentro del MÓDULO 2: S. V. B.

4. Inicio del proceso de recuperación de información.

Como evento particular para esta etapa, la presencia del MÓDULO 6: S. H. B. V. proporcionó un ambiente sólido para la extracción segura de datos. Durante este procedimiento, la información fue extraída completa y exitosamente de la unidad analizada y, en específico, del volumen estudiado sin que se lograsen filtrar copias maliciosas del código vírico pertenecientes a la partición secundaria adyacente. Así mismo, la unidad de DDE con información a recuperar soportó el procedimiento completo y, en

adición, no experimentó fallos lógicos y/o mecánicos identificables relacionados al estrés físico (eléctrico y mecánico) al que fue sometido.

Una vez concluido el procedimiento de recuperación de información y mediante la utilización del explorador de archivos, se procedió a corroborar la integridad y existencia de la información en la unidad destinada a almacenarla. El volumen “R:” contiene una copia completa de la información original contenida en la dirección “F:\Documents and Settings”; por lo tanto, **la recuperación de información ha sido lograda en esta unidad de DDE.**

- **FASE 5: COMPROBACIÓN Y ANÁLISIS DE RESULTADOS:**

La información fue ejecutada por medio de la utilización de los *softwares* asociados a las extensiones mismas de los archivos, de igual forma, estos se encontraban sin corromper y con el avance (modificaciones realizadas por el usuario) desarrollado previo al proceso infeccioso debido a virus informáticos tipo “troyano” y posterior a la recuperación virtual ejecutada por el programa “FERCUVILL V5.0”.

Las extensiones identificadas en este volumen son las siguientes: “.doc”, “.docx”, “.jpg”, “.mp4”, “.xls”, “.xlsx”, y “.pptx”, “.bmp”, “.png”, “.mpg”,

4.2.3 CASO DE RECUPERACIÓN 3

- **FASE 1: PRESENTACIÓN DEL OBJETO ANALIZADO:**

CARACTERÍSTICAS LÓGICAS IDENTIFICABLES:

1. Existe una incapacidad de la unidad de DDE para ser identificada por los *softwares*: BIOS, “*diskmgmt.msc*” y “*explorer.exe*”.
2. El dispositivo, de acuerdo a su último registro de funcionamiento, está compuesto por una partición primaria única, la cual, contiene la información del SO y del usuario.
3. Se desconocen las condiciones previas bajo las cuales la unidad se encontraba operando (SO y programas instalados, existencia de *softwares* tipo “virus informáticos”, zonas del AU y/o AS con defecto estructural).

4. La tecnología S.M.A.R.T. no pudo ser obtenida en esta unidad.

CARACTERÍSTICAS MECÁNICAS IDENTIFICABLES:

1. Los datos de placa (y lógicos) para la unidad analizada son presentados en la tabla 28 del presente proyecto de investigación (ver página 121).
2. Al ser energizado, la unidad presenta sonidos internos producidos por el motor, el cual, intenta girar pero es bloqueado súbitamente por sus rodamientos; esta característica es consistente con un deterioro en la viscosidad del medio fluido.
3. De acuerdo a la información proporcionada por el usuario de la unidad, esta fue expuesta de forma prolongada a condiciones de intemperie y, principalmente, a humedad constante.
4. La unidad, originalmente, contaba con un protector y/o “cubierta” de motor, esta última tuvo que ser removida con el fin de poder aplicar la técnica expuesta en el caso de estudio 2.2.1 del presente proyecto de investigación.

La condición predominante en esta unidad puede producir múltiples daños mecánicos y lógicos en la estructura de datos interna, sin embargo y para enmarcar una recuperación de datos efectiva, es necesario extraer (con la mayor velocidad estable posible) la información contenida y guardarla dentro de otra unidad externa, a la cual, se le podrán aplicar distintos procedimientos posteriores tales como: limpieza y desinfección de código vírico.

Este proceso de recuperación de datos dependerá básicamente de las siguientes condiciones:

1. Lograr establecer comunicación entre el módulo *firmware* instalado en la memoria ROM de la TCI con el segundo módulo *firmware* alojado en los platos magnetizables.
2. Es obligatorio que se cumplan las condiciones lógicas y mecánicas establecidas en la tabla 48.

- **FASE 2: IDENTIFICACIÓN DEL TIPO DE FALLA PREDOMINANTE:**

Esta unidad de DDE está experimentado un **fallo lógico-mecánico a causa de una condición mecánica**. Sus estructuras constitutivas y mutuamente dependientes están deterioradas de forma completa y permanente.

- **FASE 3: ANÁLISIS SOBRE LA VIABILIDAD DE LA UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0”:**

Por definición, de forma directa no puede aplicarse el *software* desarrollado pues, como ya se ha establecido, no existen el conjunto de características lógicas y mecánicas debidas para considerar el método planteado. Sin embargo, esta unidad fue intervenida temporalmente de forma tal (a partir de la utilización de herramientas externas) que se logró restablecer el movimiento de los rodamientos del motor eléctrico mediante la aplicación de energía calorífica dirigida (ver página 121); con ello se desencadenaron los proceso lógicos de identificación de los *softwares* BIOS y *firmware* correspondientes, por lo tanto, se establece que este dispositivo tiene un funcionamiento tal que se le permite clasificarlo como un candidato para la aplicación el método propuesto de recuperación de información mediante la intervención lógica del *software* “FERCUVILL V5.0”.

- **FASE 4: UTILIZACIÓN DEL *SOFTWARE* “FERCUVILL V5.0” (MÓDULOS ESPECÍFICOS):**

CONSIDERACIONES DURANTE ESTA ETAPA:

1. Los pasos y procedimiento especificados en el caso de estudio 2.2.1 son aplicados de forma periódica durante la ejecución del módulo asociado a la extracción de información.
2. El DDE no debe de experimentar ningún cambio en la posición de trabajo, de lo contrario se podría provocar un contacto entre el cabezal y los discos rígidos.
3. Se utilizará el *software*: **MÓDULO 3: I. C. B.** para efectuar el proceso de extracción de datos pues, como ya se mencionó previamente, este cuenta con una tecnología de recuperación especial para unidad de DDE inestables.

La unidad de DDE a recuperar fue acoplada y conectada al equipo computacional “huésped” mediante la utilización sus puertos nativos tipo IDE. Así mismo, se conectó una unidad de DDE en la cual se resguardó la información obtenida; para esta última, sus datos de placa (y lógicos) con presentados a continuación en la tabla 52.

DATOS DE PLACA	DESCRIPCIÓN
MARCA.	SEAGATE.
MODELO.	ST3160815AS.
DBL.	321672960 SECTORES.
INTERFAZ.	SATA.
CAPACIDAD DE ALMACENAMIENTO.	160 GB.
DATOS LÓGICOS	DESCRIPCIÓN
VOLÚMENES CONTENIDOS.	1 DISCO LÓGICO (UNIDAD “K:”).

Tabla 52. Datos de placa (y lógicos) para DDE “DESTINO” utilizado en el proceso de extracción de información mediante el MÓDULO 3: I. C. B.

APLICANDO EL MÓDULO 3: I. C. B.

De acuerdo a su descripción y características de funcionamiento, este *software* primario permite ejecutar un proceso de recuperación de información seguro en unidades mecánica y lógicamente inestables.

1. Ejecutar la venta principal de operación del MÓDULO 3: I. C. B. (figura 68).
2. Seleccionar la opción identificada como “INICIAR MÓDULO”.
3. En la ventana emergente de ambiente MS-DOS, seleccionar los campos “DISCO_1” y “DISCO_2” con los argumentos siguientes (figura 129).

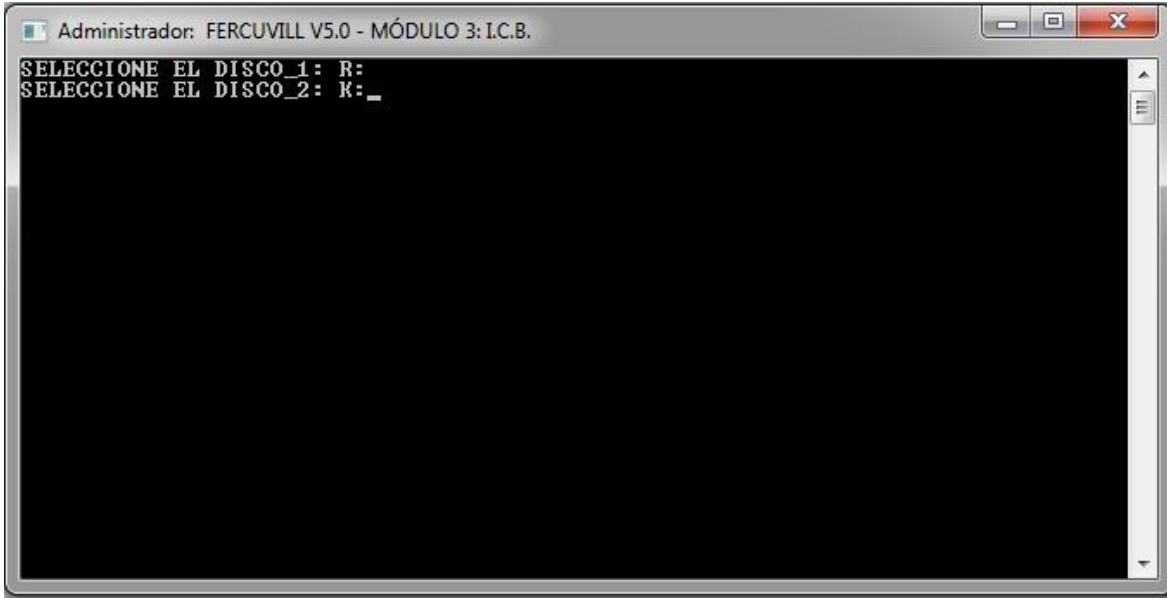


Figura 129. Visualización de la ventana emergente del MÓDULO 3: I. C. B. y selección de los argumentos “DISCO_1” y “DISCO_2”.

4. Presionar la tecla “ENTER”, verificar que la información especificada en la consola externa sea la correcta, seleccionar la opción deseada y comenzar el procedimiento (figura 130):

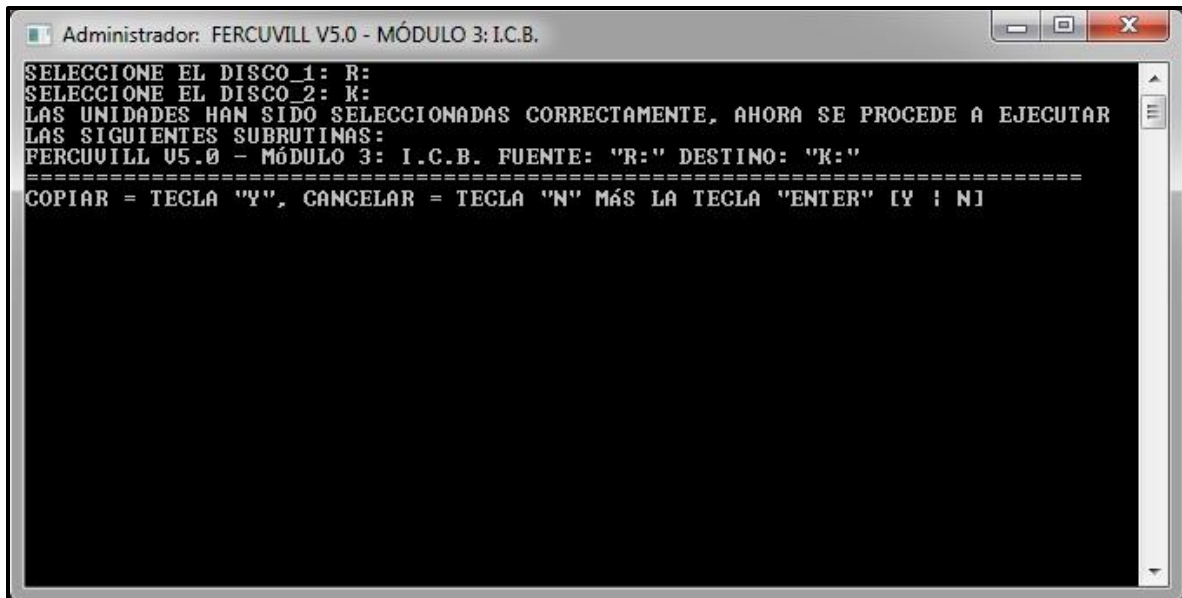


Figura 130. Visualización de la consola externa para una recuperación de datos en una ubicación “FUENTE” y “DESTINO” establecidos y específicos.

5. Una vez finalizado el proceso, se recibieron los mensajes por parte del *software* primario utilizado (figuras: 72 y 73), posteriormente, la consola fue cerrada manualmente y la unidad de DDE inestable fue suprimida de su fuente calorífica principal.
6. El DDE utilizado como “DISCO_2” fue sometido a análisis y procedimientos de desinfección de código malicioso logrando eliminarse así variantes modificadas de “virus de programa”.

OBSERVACIONES DURANTE LA ETAPA:

A continuación, en la tabla 53, se colocan los datos y comportamientos observados durante la ejecución del procedimiento de recuperación de datos aplicado:

ELEMENTO	DESCRIPCIÓN
VELOCIDAD DE EXTRACCIÓN.	EL VALOR PROMEDIO OBSERVADO EN ESTA UNIDAD OSCILÓ ENTRE LOS 89 Y 90 MB POR MINUTO.
COMPORTAMIENTOS DEL DISCO LÓGICO “R:”.	<ul style="list-style-type: none"> • EL DISPOSITIVO FUE OPERADO DE FORMA CONSTANTE DURANTE UN PERIODO DE TIEMPO IGUAL A 3.154 HORAS SIN EXPERIMENTAR PROBLEMAS RELACIONADOS A LOS RODAMIENTOS. • EL <i>SOFTWARE</i> “<i>DISKMGMT.MSC</i>” MANTUVO CONEXIÓN DIRECTA CON LA UNIDAD, EN TANTO QUE “<i>EXPLORER.EXE</i>” PRESENTÓ INTERMITENCIA EN SU FUNCIONAMIENTO.
COMPORTAMIENTOS DEL DISCO LÓGICO “K:”.	<ul style="list-style-type: none"> • ESTE DDE SOPORTÓ EFICIENTEMENTE EL PROCESO DE RECUPERACIÓN DE INFORMACIÓN Y. EN ADICIÓN, PERMITIÓ LA APLICACIÓN COMPLEMENTARIA DE UN ANÁLISIS Y PROCESOS DE

	<p>DESINFECCIÓN DE CÓDIGOS VÍRICOS EN SU PARTICIÓN PRINCIPAL.</p> <ul style="list-style-type: none"> • LA COMUNICACIÓN DE ESTA UNIDAD A TRAVÉS DE LOS <i>SOFTWARES</i> “<i>DISKMGMT.MSC</i>” Y “<i>EXPLORER.EXE</i>” FUE PERMANENTE.
<p>ESTADO DE LA RECUPERACIÓN.</p>	<ul style="list-style-type: none"> • LOS DATOS FUERON MANIPULADOS Y EXTRAÍDOS DE FORMA SEGURA. • LA RECUPERACIÓN DE LA UNIDAD FUE COMPLETA, ES DECIR, TODAS LAS LOCALIDADES FUERON RESPALDAS Y, DE ACUERDO AL USUARIO, SU INFORMACIÓN SE ENCONTRÓ ÍNTEGRA Y COMPLETA. • POSTERIOR A LA ELIMINACIÓN Y DESINFECCIÓN DE OBJETOS EN EL VOLUMEN, LA INFORMACIÓN FUE ACCESIBLE Y NO PRESENTÓ NINGÚN BLOQUEO Y/O DEGRADACIÓN LÓGICA.

Tabla 53. Comportamientos y características de operación observados en las unidades de DDE sometidas a un proceso de recuperación de datos mediante el MÓDULO 3: I. C. B.

En función de lo observado durante el proceso desarrollado y lo planteado en las tablas (30 y 53) del presente proyecto, se determinó que **el marco de recuperación de información ha sido logrado en esta unidad de DDE.**

❖ FASE 5: COMPROBACIÓN Y ANÁLISIS DE RESULTADOS:

La información recuperada en el volumen fue ejecutada por los *softwares* asociados a cada una de las extensiones presentes en la unidad; así mismo, esta fue sometida a un análisis completo configurado para desinfección y eliminación forzada de código malicioso; con ello, se logró establecer un ambiente estable de operación y edición de datos.

Las extensiones identificadas en esta unidad son las siguientes: “.doc”, “.docx”, “.jpg”, “.bmp”, “.xls”, “.xlsx”, “.bcf”, “.cer”, “.mpv2”, “.mp3.”, “.txt”, “.pdf.”, “.lha.” y “.cda”.

CONCLUSIONES PARCIALES

En este capítulo se estudiaron y aplicaron las distintas etapas conformantes del método de recuperación de información propuesto a unidades de DDE afectadas en sus diferentes estructuras constitutivas “mecánica y lógica” mediante la utilización del *software* de diseño “FERCUVILL V5.0”, así mismo, se observaron los comportamientos y resultados obtenidos y, a su vez, la relación directa existente entre estos y la información recuperada.

Este método es la arquitectura base del principio de funcionamiento del *software* “FERCUVILL V5.0” mismo, sobre este, se plantean las bases de operación y ejecución de las distintas tecnologías, herramientas y módulos disponibles orientados al restablecimiento virtual de los medios encargados de editar, leer y escribir información en unidades de DDE.

CONCLUSIONES GENERALES

Dentro de un escenario de recuperación de información existen condiciones de operación de naturaleza mecánica y/o lógica que tienden a deteriorar el medio en que se almacena la información (por ejemplo unidades de DDE) e imposibilitar el acceso a ésta. Básicamente, los daños mecánicos se deben al desgaste y envejecimiento progresivo del material constitutivo de los elementos de soporte internos de la carcasa, en tanto que los lógicos se relacionan directamente a las corrupciones virtuales (deterioro por *software* malicioso y/o daños a las estructuras del AS, AU y módulo *firmware*), de programación y operaciones destructivas desencadenadas por elementos internos y externos compuestos por fallos mecánicos y/o lógicos.

El *software* diseñado y el método de recuperación de información propuestos ofrecen una opción alterna que permite ejecutar un proceso de extracción de datos de forma segura y consistente, el cual, a su vez, no compromete la integridad física ni virtual de la unidad intervenida. La utilización del programa “FERCUVILL V5.0” representa una ventaja, ya que, de forma integral, indica el estado de funcionamiento de la unidad “huésped” y, de no encontrarse esta última en condiciones óptimas de funcionamiento, informará al usuario y ejecutará una instrucción de cierre automático con la finalidad de no agravar el deterioro identificado.

La evolución y avances tecnológicos constantes en el campo del resguardo de la información, así como los nuevos métodos de destrucción de datos provocados por los virus informáticos exigen nuevas y más complejas *softwares* de edición y manipulación de las diferentes unidades de almacenamiento y, por supuesto, de su contenido informático. Por ello, el *software* “FERCUVILL V5.0” es una respuesta real ante la necesidad de controlar, tratar y suprimir los efectos adversos a los cuales la información puede ser sometida, degradada y destruida.

El programa descrito es especialmente eficaz para efectuar las maniobras de recuperación de información en unidades con degradación lógica debido a la influencia y operación permanente de código malicioso, sin embargo, no es un programa tipo “antivirus”, por lo que debe de complementarse con la utilización de otro *software* diseñado especialmente

para la eliminación y/o desinfección de amenazas de código vírico asidos de la información recuperada, de lo contrario, el proceso destructivo continuaría en esta nueva ubicación, haciendo del proceso inicial de extracción de datos un evento inútil.

Los procedimientos de reparación lógicos y mecánicos deben de entenderse como de carácter temporal y sólo para la recuperación de información y no como un método de reparación permanente de la unidad física intervenida.

El diseño del programa permite un criterio de compatibilidad general con cualquier dispositivo de almacenamiento de información que cuente con un SA, interfaz de conexión física e identificación lógica aceptados dentro de su código de programación, por lo cual su aplicación se extiende a otros dispositivos digitales más allá del DDE.

Finalmente, “FERCUVILL V5.0” puede ser empleado dentro de otro marco y método de recuperación de información con características diferentes al planteado en la presente tesis, sin embargo, deben de respetarse los criterios de operación para los cuales fue diseñado; sólo de esa forma se garantizará que este no afecte negativa y colateralmente las diferentes muestras u objetos analizados.

ÍNDICE DE FIGURAS

Figura	Descripción	Página
1	Cubierta y datos de placa de un DDE.	14
2	Elementos internos de la carcasa.	14
3	Componentes de la TCI de un DDE con interfaz SATA.	16
4	Conector SATA de datos.	21
5	Conector SATA de alimentación.	21
6	Motor, base y eje central de DDE.	24
7	Plato magnetizable interno de un DDE.	27
8	Grabado paralelo de datos.	30
9	Grabado ortogonal de datos.	31
10	Acercamiento en el cabezal para un DDE modelo ST-251. Tomado de: [44].	34
11	Cabezas en zona de estacionamiento (1).	39
12	Cabezas en la zona de estacionamiento (2).	39
13	Distribución física del deslizador.	40
14	Brazo, cable plano de datos y bobina principal para un DDE	41
15	Comportamiento del circuito preamplificador durante la escritura de datos.	42
16	Comportamiento del circuito preamplificador durante la lectura de datos.	43
17	Distribución y arreglo lógico dentro del DDE. Tomado de: [26].	48

18	Unidad de <i>hardware</i> completa de un DDE.	53
19	Visualización en entorno MS-DOS de un disco lógico identificado como “C:”	54
20	Distribución, expresada en bytes, de la tabla de particiones para el sector RAP.	58
21	Estructura interna para el SA tipo NTFS.	61
22	Visualización de mensaje de error para un fallo en la lectura en el sector de inicio.	68
23	Visualización de mensajes de error para fallas en la firma “0XAA55” del sector RAP (2).	68
24	Visualización de datos de placa del DDE dañado por degradación en el sector RAP.	69
25	Visualización del DDE a través del <i>software</i> “ <i>diskmgmt.msc</i> ” por corrupción en el sector RAP.	72
26	Visualización del DDE a través del <i>software</i> “ <i>diskmgmt.msc</i> ” por corrupción en el sector RAP (reparado).	73
27	Visualización de la solicitud del SO para formatear una tabla de particiones vulnerada.	74
28	Visualización del mensaje de error por incompatibilidad en el SA instalado.	74
29	Distribución, expresada en bytes, de la tabla de particiones.	75
30	Utilización de particiones adyacentes activas para la identificación de un volumen dañado.	77
31	Visualización del volumen lógico a través del <i>software</i> “ <i>diskmgmt.msc</i> ” para un daño consistente en la tabla de particiones.	78
32	Datos de placa del DDE con daño consistente en la tabla de particiones.	79
		81

33	Visualización del volumen lógico a través del <i>software</i> “ <i>diskmgmt.msc</i> ” para una restauración exitosa por daño consistente en la tabla de particiones.	
34	Visualización del volumen lógico a través del <i>software</i> “ <i>explorer.exe</i> ” para una restauración exitosa por daño consistente en la tabla de particiones; inaccesible por causa de <i>software</i> malicioso.	81
35	Visualización del mensaje de advertencia del SO ante la incapacidad de eliminar un archivo malicioso.	89
36	Interfaz de control principal para el <i>software</i> “Antivirus 2010”. Tomado de: [67].	94
37	Visualización del mensaje de estado de error al abrir un archivo de extensión “.docx” deteriorado por la acción de <i>software</i> tipo “ERS”.	101
38	Visualización del estado de corrupción del <i>software</i> BIOS infectado por causa de <i>software</i> malicioso del tipo “inicio”. Tomado de: [66].	104
39	Visualización del motor de eje central con impedimento para girar debido al deterioro de las propiedades físicas del fluido viscoso.	124
40	Posicionamiento del DDE con la cara anterior expuesta.	127
41	Recubrimiento del DDE con papel tipo aluminio y exposición del área que contiene al motor.	127
42	Adaptador de 6 milímetros para pistola de aire caliente.	18
43	Instalación del adaptador y aseguramiento físico del mismo en contra de la pistola de aire caliente.	129
44	Ajuste de temperatura y reposo de en la pistola de aire caliente operada en vacío.	129
45	Posicionamiento del DDE, pistola de aire caliente y adaptador colocados de forma paralela.	130
46	Visualización de mensajes de error para un DDE con sectores de inicio dañados físicamente.	133
		134
	Visualización del mensaje de error para una demora en los procesos de	

47	escritura de datos.	
48	Visualización del mensaje en pantalla para un error de redundancia cíclica durante el proceso de copiado de información.	134
49	Visualización del mensaje de error durante el acceso a un volumen dañado.	135
50	Datos de placa para un DDE con sectores físicamente dañados.	136
51	Visualización de una condición de fisura por contacto estático en el borde exterior del disco rígido.	140
52	Acercamiento para una condición de rayado físico por contacto dinámico dentro de un DDE.	141
53	Datos de placa para DDE con daño físico por contacto dinámico del cabezal con el disco rígido.	142
54	Múltiple patrón de rayado circular en la superficie del disco rígido por contacto dinámico en un DDE.	144
55	Ventana de inicio principal del programa “FERCUVILL V5.0”.	157
56	Ventana de control de acceso por autenticación de identidad, MÓDULO 0: J.J.B.V del <i>software</i> “FERCUVILL V5.0”.	157
57	Mensaje del sistema (1): mostrado por la incorrecta especificación de los campos de acceso.	159
58	Ventana de control para carga de elementos y acceso por verificación de texto, MÓDULO 1: I.C.V.	161
59	Mensaje del sistema (2): para una carga exitosa de los elementos.	162
60	Mensaje del sistema (3): para una carga incorrecta de los elementos.	163
61	“VENTANA DE AYUDA” del MÓDULO 1: I.C.V. para acceso a la aplicación principal.	163
62	Ventana principal de operación del <i>SOFTWARE</i> MEDULAR.	164
63	Ventana principal de operación del <i>software</i> primario S.V.B.;	166

	visualización de “FUNCIONES” e “INSTRUCCIONES”.	
64	Mensaje del sistema (4): para iteración entre las unidades de “FUENTE” y “DESTINO”.	167
65	Ventana secundaria para selección de ruta “FUENTE” del volumen seleccionado.	168
66	Ventana secundaria para selección de ruta de “DESTINO” del volumen dispuesto.	168
67	Ejemplo para la selección de una “FUENTE” y “DESTINO” en el MÓDULO 2: S.V.B. para un respaldo de información entre un volumen y un DDE externo.	169
68	Interfaz gráfica de operación para el MÓDULO 3: I. C. B.; visualización de “FUNCIONES” e “INSTRUCCIONES”.	170
69	Interfaz de la consola externa principal del MÓDULO 3: I. C. B. para extracción de datos.	171
70	Selección del argumento “DISCO_1”.	172
71	Selección del argumento “DISCO_2”.	172
72	Mensaje del sistema (5): para el inicio del proceso de extracción de información.	173
73	Mensaje del sistema (6): para la notificar la finalización del proceso de extracción de información.	173
74	Selección del argumento “DISCO_1” y “DISCO_2” con el mismo valor (reiteración) y visualización del mensaje en el <i>software</i> .	174
75	Mensaje del sistema (7): solicitud de respaldo.	175
76	Mensaje del sistema (8): sugerencias de <i>software</i> .	175
77	Interfaz gráfica de operación para el MÓDULO 4: V. H. B. V.; visualización de: “FUNCIONES”, “ASISTENTE AVANZADO DE INICIO”, “MÓDULOS DE RESTAURACIÓN”, “SOFTWARES AVANZADOS” y “VENTANA DE AYUDA”.	176
78	Mensaje del sistema (9): para advertir sobre el apagado del equipo.	177

79	Mensaje del sistema (10): para advertir sobre el reinicio del equipo.	177
80	Mensaje del sistema (11): para anular un proceso de apagado/inicio.	178
81	Ventana de operación del MÓDULO 4: V. H. B. V. para la consola de restauración.	178
82	Mensaje del sistema (12): para un error en la solicitud de datos.	179
83	Mensaje del sistema (13): para indicar la activación de los módulos.	179
84	Mensaje del sistema (14): para indicar la desactivación de los módulos.	179
85	Interfaz gráfica de operación para el MÓDULO A: K. L. G.; visualización de “FUNCIONES”, “INSTRUCCIONES” e “INFORMACIÓN DE LA UNIDAD”.	180
86	Interfaz gráfica de operación para el MÓDULO B: A. J. L.; visualización de “INSTRUCCIONES”, “RUTA DE LOS OBJETOS”, “PROGRESO GENERAL” y “BOTONES DE CONTROL”.	181
87	Mensaje del sistema (15): para un estado de protección activo de un objeto específico.	183
88	Mensaje del sistema (16): para un estado de protección inactivo de un objeto específico.	183
89	Interfaz gráfica de operación para el MÓDULO 5: P. A. H.; visualización de “INSTRUCCIONES”, “RUTA DE LOS OBJETOS”, “PROGRESO GENERAL” y “BOTONES DE CONTROL”.	184
90	Mensaje del sistema (17): para la activación completa de la herramienta seleccionada.	185
91	Mensaje del sistema (18): para la desactivación completa de la herramienta seleccionada.	185
92	Interfaz gráfica de operación del MÓDULO 5: P. A. H. para la ejecución del <i>software</i> “DEPURADOR”.	186
93	Interfaz gráfica de operación para el MÓDULO 6: S. H. B. V.	188
94	Mensaje del sistema (19): solicitud de continuación y reinicio del sistema.	189

95	Mensaje del sistema (20): sugerencia de reinicio del sistema.	189
96	Interfaz gráfica de operación para el MÓDULO 7: H. A. A B., visualización de elementos.	190
97	Interfaz de la consola externa principal del MÓDULO 7: H. A. A B. para el desbloqueo de datos.	191
98	Mensaje del sistema (21): para visualizar íntegramente el contenido de un disco lógico.	192
99	Mensaje del sistema (22): para la recuperación de volúmenes completos de datos.	192
100	Mensaje del sistema (23): para la ejecución de un reinicio del sistema.	193
101	Mensaje del sistema (24): para visualizar la letra asociada al volumen lógico.	193
102	Selección de la unidad lógica descrita por el argumento "D:" como aquella a ser modificada por la consola externa.	193
103	Ejecución de las etapas de desbloqueo de información sobre el objeto especificado como "D:" mediante la utilización de la consola externa.	194
104	Mensaje del sistema (25): notifica la intervención segura del disco lógico analizado.	194
105	Mensaje del sistema (26): para ejecutar un respaldo de la información reparada.	195
106	Mensaje del sistema (27): sugerencia para la extracción de datos.	195
107	Selección del argumento "H:" como unidad de destino (inexistente) y visualización del mensaje en <i>software</i> .	195
108	Visualización del contenido del volumen lógico "G:" posterior al proceso de desinfección.	211
109	Ventana de principal de operación del MÓDULO 7: H. A. A B.	212
		213
110	Consola principal de operación en ambiente MS-DOS del MÓDULO 7: H. A. A B.	

111	Selección de la unidad lógica descrita por el argumento “G:” como aquella a ser modificada por la consola externa.	213
112	Ejecución de las etapas de desbloqueo de información sobre el objeto especificado como “G:” mediante la utilización de la consola externa.	214
113	Visualización del volumen lógico “G:” a través del <i>software</i> “ <i>explorer.exe</i> ” para una intervención exitosa del MÓDULO 7: H. A. A. B.	214
114	Establecimiento de los parámetros “FUENTE” y “DESTINO” dentro del MÓDULO 2: S. V. B.	215
115	Ventana de progreso para un proceso de extracción de datos iniciado por el MÓDULO 2: S. V. B.	216
116	Visualización del directorio principal contenedor de información del usuario en el volumen “F:” posterior al proceso de desinfección y eliminación forzada de <i>software</i> malicioso.	220
117	Ventana de principal de operación del MÓDULO 7: H. A. A. B.	221
118	Consola externa de operación en ambiente MS-DOS del MÓDULO 7: H. A. A. B.	222
119	Selección de la unidad lógica descrita por el argumento “F:” como aquella a ser modificada por la consola externa.	223
120	Ejecución de las etapas de desbloqueo sobre el objeto especificado como “F:” mediante la utilización de la consola externa.	223
121	Visualización del volumen lógico “F:” a través del <i>software</i> “ <i>explorer.exe</i> ” para una intervención completa del MÓDULO 7: H. A. A. B.	224
122	Visualización de error en pantalla por acceso fallido debido a la usencia de permisos administrativos en el volumen “F:”.	224
123	Interfaz gráfica de operación para el MÓDULO 5: P. A. H.; visualización de “INSTRUCCIONES”, y “BOTONES DE CONTROL”.	225
124	Selección de la característica “FORZAR PROPIEDAD” en un directorio específico para un restablecimiento de las propiedades administrativas de un objeto particular.	226
125	Visualización de un disco lógico posterior a la aplicación del MÓDULO 5: P. A. H. para la obtención de propiedades administrativas	226

en un directorio particular.

126	Interfaz gráfica de operación para el MÓDULO 6: S. H. B. V.	227
127	Mensaje del sistema (19): solicitud de continuación y reinicio del sistema.	228
128	Establecimiento de los parámetros “FUENTE” y “DESTINO” dentro del MÓDULO 2: S. V. B.	229
129	Visualización de la ventana emergente del MÓDULO 3: I. C. B. y selección de los argumentos “DISCO_1” y “DISCO_2”.	234
130	Visualización de la consola externa para una recuperación de datos en una ubicación “FUENTE” y “DESTINO” establecidos y específicos.	234

ÍNDICE DE TABLAS

Tabla	Descripción	Página
1	Evolución y fusión de fabricantes de dispositivos de DDE.	9 - 10
2	Elementos mecánicos y lógicos estructurales del DDE.	12
3	Subdivisión de los elementos mecánicos del DDE.	13
4	Identificación de los elementos de la carcasa y cubierta del DDE.	15
5	Distribución física de los componentes de la TCI.	16
6	Identificación de los componentes de la TCI.	17
7	Valores de nodos para el conector SATA de datos.	22
8	Valores de nodos para el conector SATA de alimentación.	23
9	Componentes del motor del DDE.	25
10	Elementos constitutivos del plato magnético.	29
11	Estructura física de los tipos de grabado magnético.	33
12	Identificación de los elementos constitutivos del cabezal.	35
13	Elementos constitutivos del deslizador.	41
14	Organización jerárquica de la estructura lógica en el DDE.	45 – 46
15	Elementos constitutivos de la organización lógica del DDE.	52
16	Estructura lógica del sector RAP.	57
17	Estructura lógica de la zona FAT en el SA FAT32.	64 – 65
18	Datos de placa para DDE con degradación del sector RAP.	70
19	Componentes del sector RAP, tipo de daño, método de reparación	73

	aplicado y resultados obtenidos.	
20	Datos de placa para DDE con daño consistente en la tabla de particiones.	79
21	Componentes de la tabla de particiones, errores, método de solución y resultados.	83
22	Arreglo estandarizado para los elementos estructurales del SO.	85 – 88
23	Clasificación general de los tipos de virus informáticos actuantes en el SO.	91
24	Datos de placa del conjunto de unidades de DDE utilizados para el estudio de daños lógicos a causa de softwares identificados del tipo “virus informático”.	112
25	Distribución física y lógica de los códigos maliciosos en cada DDE anfitrión analizado.	113
26	Aplicación de métodos de desinfección y eliminación de software vírico; obtención de resultados.	115
27	Tendencias, comparaciones y estadísticas de sistemas computacionales sin protección antivirus y/o desactualizada.	120
28	Datos de placa para DDE con degradación del fluido viscoso presente en los rodamientos de motor de eje central.	125
29	Identificación de elementos externos y puntos de conexión para un motor de DDE.	126
30	Motor eléctrico y sus rodamientos, tipo de daño, método de solución y resultados.	132
31	Datos de placa para DDE con sectores dañados físicamente.	137
32	Errores, observaciones y resultados obtenidos para un DDE con daños físicos en sectores.	139
33	Datos de placa (y lógicos) para DDE afectado físicamente en su disco rígido por contacto dinámico.	143
34	Errores, observaciones y resultados obtenidos en un DDE con daños físicos en los platos magnetizables.	145

35	Recursos físicos y lógicos mínimos de un sistema computacional para la instalación y ejecución del software “FERCUVILL V5.0”.	148
36	Descripción de los elementos estructurales de la ventana de inicio del software “FERCUVILL V5.0”.	159
37	Descripción de los elementos estructurales del MÓDULO 0: J.J.C.V del software “FERCUVILL V5.0”.	160
38	Descripción de los elementos estructurales del MÓDULO 1: I.C.V. del software “FERCUVILL V5.0”.	163
39	Descripción de los elementos estructurales del SOFTWARE MEDULAR.	166
40	Descripción de los elementos estructurales del MÓDULO 2: S.V.B. del software “FERCUVILL V5.0”.	168
41	Descripción de los elementos estructurales del MÓDULO 3: I .C .B. del software “FERCUVILL V5.0”.	172
42	Comportamiento, mensajes y opciones de configuración para un caso de iteración en los parámetros “DISCO_1” y “DISCO_2”.	176
43	Descripción de los elementos estructurales del MÓDULO B: A. J. L. del software “FERCUVILL V5.0”.	183
44	Descripción de los elementos estructurales del MÓDULO 5: P. A. H. para la ejecución del software “DEPURADOR”	188
45	Descripción de los elementos estructurales del MÓDULO 7: H. A. A. B. (interfaz gráfica y consola externa de operación) del software “FERCUVILL V5.0”.	192 – 193
46	Clasificación de las causas y consecuencias detectables en un DDE por influencia de las fallas mecánicas y lógicas expuestas.	200 - 204
47	Comportamientos generales característicos para las fallas mecánicas y lógicas pertenecientes a un DDE.	205
48	Condiciones físicas y lógicas necesarias para utilizar el software “FERCUVILL V5.0” dentro de un marco de recuperación de información en unidades de DDE.	206
49	Datos de placa y lógicos para DDE “DESTINO” utilizado en el proceso de extracción de información mediante el MÓDULO 2: S. V. B.	216

50	Datos de placa y lógicos para un DDE deteriorado en su volumen principal por causa de amenazas tipo “troyano”.	219
51	Datos de placa y lógicos para DDE “DESTINO” utilizado en el proceso de extracción de información mediante el MÓDULO 2: S. V. B.	230
52	Datos de placa (y lógicos) para DDE “DESTINO” utilizado en el proceso de extracción de información mediante el MÓDULO 3: I. C. B.	234
53	Comportamientos y características de operación observados en las unidades de DDE sometidas a un proceso de recuperación de datos mediante el MÓDULO 3: I. C. B.	236 - 237

REFERENCIAS

- [1] Ace Data Recovery. (s/f). *Hard Drive Data Recovery: Inside Hard Disk Drives Part 1*. Datarecovery. Recuperado de:
<http://www.datarecovery.net/articles/inside-hard-disk-drive-part1.aspx>
Consultado 5 June 2015
- [2] Ace Data Recovery. (s/f). *Hard Drive Data Recovery: Inside Hard Disk Drives Part 2*. Datarecovery. Recuperado de:
<http://www.datarecovery.net/articles/inside-hard-disk-drive-part2.aspx>
Consultado 5 June 2015
- [3] Anderson, D. (s/f). *The top hard drive companies in the world*. Southjerseydata. Recuperado de:
<http://www.southjerseydata.com/hard-drive-manufacturers.html>
Consultado 12 febrero 2015
- [4] Al Mamum, A., Guo, G., y Bi, C. (2007). *Hard Disk Drive: Mechatronics and Control*. Texas: CRC Press.
- [5] AllPinouts. (s/f). *Serial ATA (SATA, Serial Advanced Technology Attachment)*. AllPinouts. Recuperado de:
http://www.allpinouts.org/index.php/Serial_ATA_%28SATA,_Serial_Advanced_Technology_Attachment%29
Consultado 26 abril 2013
- [6] Ascii. (s/f). *Caracteres estándares*. Tabla de códigos Ascii. Recuperado de:
<http://ascii.cl/es/>
Consultado 22 octubre 2015

- [7] Avast. (s/f). *aswMBR 1.0.1.2290*. Avast. Recuperado de:
<http://public.avast.com/~gmerek/aswMBR.htm>
Consultado 16 febrero 2015
- [8] Barajas, S. (2001). *Discos duros y particiones*. Saulo.net. Recuperado de:
<http://www.saulo.net/pub/ddypart/a.htm>
Consultado 29 de abril de 2015
- [9] Behrisch, R. (1981). *Sputtering by particle bombardment*. Berlin, Alemania: Springer.
- [10] Belcher, J., Dourmashkin, P., y Liao, S. (2004). *Introduction to Electricity and Magnetism*. Massachusetts: Pearson.
- [11] Blount, W. (2007). *Fluid Dynamic Bearing Spindle Motors: Their future in hard disk drives*. HGST. Recuperado de:
https://www.hgst.com/sites/default/files/resources/FD_White_Paper_FINAL.pdf
Consultado 20 Marzo 2015
- [12] Bortnik, S. (2011). *A 25 años de Chernobyl y a 12 años del (virus) Chernobyl*. Welivesecurity. Recuperado de:
<http://www.welivesecurity.com/la-es/2011/04/26/25-anos-chernobyl-12-anos-virus/>
Consultado 17 diciembre 2014
- [13] Bortnik, S. (2010). *Tipos de heurística*. Welivesecurity. Recuperado de:
<http://www.welivesecurity.com/la-es/2010/02/16/tipos-heuristica/>
Consultado 17 diciembre 2014

- [14] Broanche, A. 2006. *Microsoft's file system patent upheld*. NCET. Recuperado de:
<http://www.cnet.com/news/microsofts-file-system-patent-upheld/>
Consultado 29 octubre 2014
- [15] Brouwer, A. (2015). *List of partition identifiers for PCs*. tue.nl. Recuperado de:
http://www.win.tue.nl/~aeb/partitions/partition_types.html#toc1
Consultado 21 noviembre 2014
- [16] Brouwer, A. (2015). *Properties of partition tables*. tue.nl. Recuperado de:
https://www.win.tue.nl/~aeb/partitions/partition_types-2.html
Consultado 21 noviembre 2014
- [17] Byte Magazine. (1983). *A Short History of MS-DOS*. Paterson Technology.
Recuperado de:
<http://www.patersontech.com/dos/byte%E2%80%93history.aspx>
Consultado 21 noviembre 2014
- [18] CCM. (2016). *Explorer: explorer.exe*. CCM High-Tech. Recuperado de:
<http://es.ccm.net/contents/461-explorer-explorer-exe>
Consultado 8 julio 2015
- [19] Charkiewicz, G. (2014). *¿Qué es un macro virus y cómo funciona?* Welivesecurity.
Recuperado de:
<http://www.welivesecurity.com/la-es/2014/06/13/que-es-macro-virus-como-funciona/>
Consultado 23 julio 2014
- [20] Chen, B., M., Lee, T., H., Peng, K., y Venkataramanan, V. (2002). *Hard Disk Drive servo System*. Londres, Reino Unido: Springer.

- [21] Christensen, C. (2010). The Rigid Disk Drive Industry: A History of Commercial and Technological Turbulence. *Business History Review*, 4(67).
- [22] *Commodore: 128 Programmer's Reference Guide*. (1986). Toronto, Canadá: Bantam Book.
- [23] Computer History Museum. (s/f). *Artifact Details*. Computer History Museum. Recuperado de:
<http://www.computerhistory.org/collections/catalog/102729821>
Consultado 30 marzo 2014
- [24] Computer History Museum. (2000). *IBM 75GXP*. Computerhistory. Recuperado de:
<http://s3.computerhistory.org/groups/ds-ibm-75gxp-family-20121031.pdf>
Consultado 28 abril 2014
- [25] Computer Hope. (s/f) *BPB*. Computer Hope. Recuerado de:
<http://www.computerhope.com/jargon/b/bpb.htm>
Consultado 18 noviembre 2011
- [26] Díaz, P. (s/f). *Estructura física y lógica del Disco Duro*. Wordpress. Recuperado en:
<https://lasir.files.wordpress.com/2010/10/estructura-del-disco.pdf>
Consultado 30 octubre 2015
- [27] Dembowski, K. (2003). *Hardware: Información sobre la totalidad del hardware de rápido acceso*. (Segunda edición). Barcelona, España: Marcombo.
- [28] Ecured. (s/f). *Seagate*. Ecured. Recuperado de:
<http://www.ecured.cu/index.php/Seagate>
Consultado 18 abril 2015

- [29] EcuRed. (s/f). *Virus polimórfico*. EcuRed. Recuperado de:
http://www.ecured.cu/Virus_polim%C3%B3rfico
Consultado 10 noviembre 2015
- [30] Fairhead, H. (2016). *Hexadecimal*. I Programmer. Recuperado de:
<http://www.i-programmer.info/babbages-bag/478-hexadecimal.html>
Consultado 16 febrero 2015
- [31] Fernández, H. (s/f). *Ecuaciones de Maxwell*. Universidad Tecnológica Nacional-Argentina. Recuperado de:
<http://www.fisica-relatividad.com.ar/temas-especiales/ecuaciones-de-maxwell>
Consultado 9 mayo 2013
- [32] Gagne, G., Galvin, P., y Silberschatz, A. (2005). *Student's manual to accompany operating system concepts*. (Séptima edición) Nueva Jersey: Wiley John Wiley & Sons. Inc. Recuperado de:
<http://pages.cs.wisc.edu/~remzi/OSTEP/>
Consultado 23 junio 2014
- [33] Gardner, T. 2012. *Rodime RO352*. ComputerHistory. Recuperado de:
<http://s3.computerhistory.org/groups/rodime-ro352.pdf>
Consultado 8 febrero 2015
- [34] Geek. (s/f). *180 GB hard drive from Seagate*. Geek. Recuperado de:
<http://www.geek.com/news/180-gb-hard-drive-from-seagate-542892/>
Consultado 4 abril 2015

- [35] Glosarioit. (s/f). *Densidad de pista - Sección Informática*. Glosarioit. Recuperado de:
http://www.glosarioit.com/#!Densidad_de_pista
Consultado 27 abril 2015
- [36] GMR Head Technology: Increased areal density and improved performance. (1999) *Western Digital Corporation*. Recuperado de:
http://isites.harvard.edu/fs/docs/icb.topic86897.files/GMR_Summary_from_Western_Digital.pdf
Consultado 21 noviembre 2013
- [37] GNU. (s/f). *¿Qué es el software libre?* GNU. Recuperado de:
<http://www.gnu.org/philosophy/free-sw.es.html>
Consultado 29 junio 2015
- [38] Govindarajalu, B. (2008). *IBM Pc and Clones: Hardware, Troubleshooting And Maintenance*. (Segunda Edición). New Delhi: Tata McGraw-Hill.
- [39] International Business Machines Corp. (s/f). *Chronological History of IBM*. IBM. Recuperado de:
https://www-03.ibm.com/ibm/history/history/history_intro.html
Consultado 08 febrero 2015
- [40] International Business Machines Corp. (s/f). *IBM 1311 disk storage drive*. IBM. Recuperado de:
https://www-03.ibm.com/ibm/history/exhibits/storage/storage_1311.html
Consultado 02 enero 2014

- [41] Kaspersky. (s/f). *What is a Boot Sector Virus?* Kaspersky. Recuperado de:
<https://usa.kaspersky.com/internet-security-center/definitions/boot-sector-virus#.VvMbq-Yx7NI>
Consultado 28 marzo 2014
- [42] Karbo, M. (s/f). *The CPU's immediate surroundings*. Karbosguide. Recuperado de:
<http://www.karbosguide.com/books/pcarchitecture/chapter17.htm>
Consultado 8 julio de 2015
- [43] Kovar, J. (2012). *The History Of The Hard Drive And Its Future*. CRN. Recuperado de:
<http://www.crn.com/slide-shows/storage/240142353/the-history-of-the-hard-drive-and-ts-future.htm/pgno/0/11>
Consultado 6 agosto 2014
- [44] Kozierok, C. (2001). *Ferrite Heads*. The pcguide. Recuperado de:
<http://www.pcguides.com/ref/hdd/op/heads/techFerrite-c.html>
Consultado 9 mayo 2013
- [45] Kozierok., C. (2001). *(Anisotropic) Magnetoresistive (MR/AMR) Heads*. The PC Guide. Recuperado de:
http://www.pcguides.com/ref/hdd/op/heads/tech_MR.htm
Consultado 21 noviembre 2013
- [46] Kozierok, C. (2001). *ST-506 / ST-412 Interface*. The PC guide. Recuperado de:
<http://www.pcguides.com/ref/hdd/if/obsoST506-c.html>
Consultado 15 marzo 2013

- [47] La Red, M. (2001). *Sistemas Operativos*. Universidad Nacional del Nordeste. Argentina. Recuperado de:
http://sistop.gwolf.org/biblio/Sistemas_Operativos_-_Luis_La_Red_Martinez.pdf
Consultado 12 julio 2015
- [48] Legitreviews. (2008). *The History of Storage[56K ALERT]*. Legitreviews. Recuperado de:
<http://forums.legitreviews.com/viewtopic.php?t=16883>
Consultado 30 marzo 2014
- [49] Long, J. (s/f). *11 Facts (About Seagate) to Stump Any History Buff*. Seagate. Recuperado de:
<http://blog.seagate.com/consumer/11-facts-about-seagate-to-stump-any-history-buff/>
Consultado 30 marzo 2014
- [50] López, L. (23 de noviembre de 2003). Boletín técnico: virus en sectores de arranque. *VSantivirus*, 1234(8). Recuperado de:
<http://www.vsantivirus.com/fdisk-mbr.htm>
Consultado 29 abril 2015
- [51] Mateos, M. (2013). *Así funcionan: sistemas de ficheros*. Genbeta. Recuperado de:
<http://www.genbeta.com/sistemas-operativos/asi-funcionan-sistema-de-ficheros>
Consultado 19 diciembre 2013

- [52] MathWorks. (s/f). *Design Hard-Disk Read/Write Head Controller*. MathWorks. Recuperado de:

http://www.mathworks.com/help/control/ug/hard-disk-readwrite-head-controller.html?s_tid=gn_loc_drop

Consultado 2 agosto 2013
- [53] MathWorks. (s/f). *Digital Servo Control of a Hard-Disk Drive*. MathWorks. Recuperado de:

<http://www.mathworks.com/help/control/examples/digital-servo-control-of-a-hard-disk-drive.html>

Consultado 2 agosto 2013
- [54] Mee, C., y Daniel, E. (1996). *Magnetic storage handbook*. Nueva York: McGraw-Hill.
- [55] Morris, M., M. (2003). *Diseño Digital*. (Tercera edición). México: Pearson Educación. Recuperado de:

http://www.academia.edu/23767225/Dise%C3%B1o_digital_3_ed-_morris_mano

Consultado 5 Junio 2015
- [56] Meisner, J. (2013). *Latest Security Intelligence Report Shows 24 Percent of PCs are Unprotected*. Microsoft. Recuperado de:

<http://blogs.microsoft.com/blog/2013/04/17/latest-security-intelligence-report-shows-24-percent-of-pcs-are-unprotected/>

Consultado 22 junio 2015

- [57] Microsoft Corporation. (2005). *Comparación de NTFS con FAT y FAT32*. Microsoft. Recuperado de:
<https://msdn.microsoft.com/es-es/library/cc779002%28v=ws.10%29.aspx>
Consultado 29 octubre 2014
- [58] Microsoft Corporation. (s/f). *Comparación de los sistemas de archivos NTFS y FAT*. Microsoft. Recuperado de:
<http://windows.microsoft.com/es-mx/windows-vista/comparing-ntfs-and-fat-file-systems>
Consultado 29 octubre 2014
- [59] Microsoft Corporation. (s/f). Explicación de CHKDSK y de los nuevos modificadores /C e /I. Microsoft. Recuperado de:
<https://support.microsoft.com/es-es/kb/187941>
Consultado 22 octubre 2015
- [60] Microsoft Corporation. (s/f). *Hard Disk Errors Caused by Damaged Data or Physical Damage*. Microsoft. Recuperado de:
<https://support.microsoft.com/en-us/kb/150532>
Consultado 10 noviembre 2015
- [61] Microsoft Corporation. (2003). *How NTFS Works*. Microsoft-TechNet. Recuperado de:
<https://technet.microsoft.com/en-us/library/cc781134%28v=ws.10%29.aspx>
Consultado 29 octubre 2014

- [62] Microsoft Corporation. (s/f). Opciones de línea de comandos de Bootsect. Microsoft-TechNet. Recuperado de:
<https://technet.microsoft.com/es-mx/library/cc749177%28v=ws.10%29.aspx>
Consultado 16 febrero 2015
- [63] Microsoft Corporation. (s/f). ¿Qué es un controlador? Microsoft. Recuperado de:
<http://windows.microsoft.com/es-mx/windows/what-is-driver#1TC=windows-7>
Consultado 22 junio 2015
- [64] Microsoft Corporation. (s/f). *What are partitions and logical drives?* Microsoft. Recuperado de:
<http://windows.microsoft.com/en-us/windows-vista/what-are-partitions-and-logical-drives>
Consultado 18 marzo 2015
- [65] Moser, A., Takano, K., Margulies, D., Albrecht, M., Sonobe, Y., Ikeda, Y., Sun, S., y Fullerton, E. (2002). Magnetic recording: advancing into the Future. *Journal of Physics D: An Applied Physics*, (35).
- [66] Nosólolinux. (2006). *El virus Chernobyl (CIH)*. Nosólolinux. Recuperado de:
<http://nosólolinux.com/2006/07/03/el-virus-chernobyl-cih/>
Consultado 15 noviembre 2013
- [67] Oregon State University. (s/f). *About Fake AntiVirus Warnings*. Oregon State University. Recuperado de:
<http://oregonstate.edu/helpdocs/safety-and-security/computer-viruses-fraud/computer-viruses/fake-antivirus-warnings>
Consultado 22 octubre 2015

- [68] Panda Security. (s/f). *Técnicas de programación y camuflaje*. Panda Security. Recuperado de:
<http://www.pandasecurity.com/mexico/homeusers/security-info/about-malware/technical-data/date-2.htm>
Consultado 10 noviembre 2015
- [69] Panda Security. (s/f). *Tipos de virus*. Panda security. Recuperado de:
<http://www.pandasecurity.com/mexico/homeusers/security-info/about-malware/technical-data/date-3.htm>
Consultado 10 noviembre 2015
- [70] Piquer, J. (1999). *Arquitectura del Sistema Operativo*. Uchile. Recuperado de:
<http://users.dcc.uchile.cl/~jpiquer/Docencia/SO/aps/node16.html>
Consultado 22 junio 2015
- [71] Puigdemunt, E. (1999). *Unidades de disco*. Pchardware. Recuperado de:
<http://pchardware.org/discos/discounidad.php>
Consultado 9 mayo 2013
- [72] *Quimitube*. (s/f). *¿El aluminio se oxida?* Quimitube. Recuperado de:
<http://www.quimitube.com/oxidacion-aluminio>
Consultado 28 abril 2015
- [73] Rodríguez, H. (s/f). *Soldadura Fuerte y Blanda*. Ingemecánica. Recuperado de:
<http://ingemecanica.com/tutorialsemanal/tutorialn49.html#seccion21>
Consultado 10 noviembre 2015

- [74] Rouse, M. (2006). *Byte*. Techtarget. Recuperado de:
<http://searchstorage.techtarget.com/definition/byte>
Consultado 29 abril 2015
- [75] Rouse, M. (2010). *EEPROM (electrically erasable programmable read-only memory)*. TechTarget. Recuperado de:
<http://whatis.techtarget.com/definition/EEPROM-electrically-erasable-programmable-read-only-memory>
Consultado 28 marzo 2014
- [76] Rouse, M. (s/f). *Trojan horse*. TechTarget. Recuperado de:
<http://searchsecurity.techtarget.com/definition/Trojan-horse>
Consultado 14 abril 2014
- [77] Rubtsov, A. (2009). *HDD from inside: Main parts*. HDDScans. Recuperado de:
http://hddscan.com/doc/HDD_from_inside.html
Consultado 15 junio 2015
- [78] Rubtsov, A. (2009). *HDD from inside: Tracks and Zones: How hard it can be?* HDDScan. Recuperado de:
http://hddscan.com/doc/HDD_Tracks_and_Zones.html
Consultado 16 mayo 2015
- [79] Seagate. (s/f). *Acerca de Seagate*. Seagate. Recuperado de:
<http://www.seagate.com/la/es/about-seagate/seagate-history/>
Consultado 17 abril 2015

- [80] Seagate. (s/f). *Archive HDD, Cold Data Cloud Hard Drive for Data Archiving*. Seagate. Recuperado de:

<http://www.seagate.com/la/es/products/enterprise-servers-storage/nearline-storage/archive-hdd/>

Consultado 15 junio 2015
- [81] Seagate, Desktop HDD (Barracuda) (2015, abril). Seagate. Recuperado de:

<http://www.seagate.com/la/es/support/internal-hard-drives/desktop-hard-drives/desktop-hdd/>

Consultado 17 abril 2015
- [82] Security Null. (2012). *4 fallos de disco duro más comunes*. Security Null. Recuperado de:

<http://www.securitynull.net/fallos-de-disco-duro-mas-comunes/>

Consultado 12 febrero 2014
- [83] Sommer, D. (marzo 14, 1988). Adoption of IBM's SAA as standard is inevitable, users say. *InfoWorld: The PC News Weekly*, 10, 73. Recuperado de:

https://books.google.com.mx/books?id=6j4EAAAAMBAJ&pg=PA73&lpg=PA73&dq=CP3022+hard+drive&source=bl&ots=Z_LrRC41Hm&sig=ohtai-LOoRV-RbqZKTmb8fVv8Pk&hl=es-419&sa=X&ei=lrGIVd24F8TyoATXrYCQCQ&ved=0CFkQ6AEwCQ#v=onepage&q=CP3022%20hard%20drive&f=false

Consultado 30 marzo 2014
- [84] Sprecher, B., Kleijn, R., y Kramer, G. (2014). Recycling Potential of Neodymium: The Case of Computer Hard Disk Drives. *American Chemical Society*, (48).

- [85] Symantec.(s/f). Volumen dinámico. Symantec. Recuperado de:
https://www.symantec.com/es/es/security_response/glossary/define.jsp?letter=d&word=dynamic-volume
Consultado: 26 septiembre 2015
- [86] Symantec. (s/f). *Worms*. Symantec. Recuperado de:
https://www.symantec.com/security_response/glossary/define.jsp?letter=w&word=worms
Consultado 14 abril 2014
- [87] Technopedia. (s/f). *Physical Drive*. Techopedia. Recuperado de:
<https://www.techopedia.com/definition/2254/physical-drive>
Consultado 30 octubre 2015
- [88] Theophanidis, P. (2013). *First Gigabyte Hard Drive: The IBM 3380 HDA*. Aphelis.
Recuperado de:
<http://aphelis.net/first-gigabyte-hard-drive-ibm-3380/>
Consultado 03 diciembre 2014
- [89] Tech Terms. *Bit*. Tech Terms. Recuperado de:
<http://techterms.com/definition/bit>
Consultado 10 noviembre 2015
- [90] Toshiba. (s/f). *Large Capacity HDD for External Storage: MQ03ABB300 / MQ03ABB200*. Toshiba. Recuperado de:
<http://toshiba.semicon-storage.com/ap-en/product/storage/products/specialty/mq03abbxxx.html>
Consultado 7 febrero 2015

- [91] Toshiba. (s/f). *Toshiba: Business to Business Integrated Solutions*. Recuperado de:
<http://www.toshiba.com/tai/>
Consultado 17 julio 2014
- [92] Universidad Autónoma de Yucatán. (s/f). *Características de los virus*. UADY.
Recuperado de:
<http://www.riuady.uady.mx/virus/caracs.php>
Consultado 22 octubre 2015
- [93] Universidad Nacional Autónoma de México. (2015). *Software y hardware para la comunidad*. Dirección General de Cómputo y de Tecnologías de Información y Comunicación. Recuperado de:
<http://www.tic.unam.mx/software.html#antivirus>
Consultado 22 octubre 2015
- [94] Utica. (s/f). *IDE/ATA Interface*. Utica. Recuperado de:
http://www.utica.edu/faculty_staff/qma/07.ATA.pdf
Consultado 26 abril 2015
- [95] Virusinformaticos. (s/f). *Virus enlace o directorio*. Virusinformaticos. Recuperado de:
<http://virusinformaticos.50webs.com/enlace.htm>
Consultado 22 octubre 2015
- [96] Vlaurie. (s/f). *Hard Disk Management in Windows XP- the Console*. Computer Education. Recuperado de:
<http://vlaurie.com/computers2/Articles/harddrive2.htm>
Consultado 29 abril de 2015

- [97] VSAntivirus. (s/f). *¿Qué es un HOAX?* VSAntivirus. Recuperado de:
<http://www.vsantivirus.com/hoaxes.htm>
Consultado 15 noviembre 2012
- [98] Wikifoundry. (2015). *Conner CP340 Family*. Wikifoundry. Recuperado de:
<http://chmhdd.wikifoundry.com/page/Conner+CP340+Family>
Consultado 30 marzo 2014
- [99] Microsoft Homepage (2015, 08). Recuperado de:
www.microsoft.com/en-us/windows
- [100] Yiwo, C. (2006). *Data Recovery e-book V1.5*. Recuperado de:
http://www.german-sales.com/Anleitung_Data_Recovery_Wizard_EN.pdf
Consultado 03 mayo 2015
- [101] ZAR. (s/f). *CHKDSK: "RAW filesystem" message*. ZAR. Recuperado de:
<http://www.z-a-recovery.com/articles/raw-filesystem.aspx>
Consultado 29 abril 2015

GLOSARIO DE SIGLAS

AAD: Áreas de Almacenamiento de Datos.

Al: Aluminio.

AS: Área de Servicio.

AU: Área de Usuario.

b: Bit.

B: Byte.

BB: Ball Bearing.

BIOS: Basic Input Output System.

BPP: Bits Por Pulgada.

C.D.: Corriente Directa.

CCS: Cilindro-Cabeza-Sector.

CI: Circuito Integrado.

Co: Cobalto.

Cobre: Cu.

DBL: Dirección del Bloque Lógico.

DDE: Disco Duro Electromecánico.

DDR SDRAM: Dual Data Rate, Synchronus Dymanic Random Access Memory.

E/S: Entrada/Salida.

EEPROM: Electrically Erasable Programmable Read Only Memory.

EPP: Error de Posicionamiento de Pista.

FAT32: File Allocation Table.

FDB: Fluid Dynamic Bearing.

GB/s: Giga Bytes sobre segundo.

GB: Giga Byte.

IPA: Interfaz de Programación de Aplicación.

KB/s: Kilo Bytes sobre segundo.

KB: Kilo Bytes.

MB: Mega Bytes.

MHz: Mega Hertz.

N: Norte.

NTFS: New Technology File System.

PBBIOS: Parámetros de Bloque del *software* BIOS.

PPP: Pistas por Pulgada.

RAM: Random Access Memories.

RAP: Registro de Arranque Principal.

RISO: Registro de Inicio de Sistema Operativo.

RPM: Revoluciones Por Minuto.

S.M.A.R.T.: Self-Monitoring, Analysis and Reporting Technology.

S: Sur.

SA: Sistema de Archivos.

SATA: Serial Advanced Technology Attachment.

SO: Sistema Operativo.

SVT: Supresor de Voltaje Transitorio.

TB: Tera Bytes.

TCI: Tarjeta de Circuito Impreso.

TMA: Tabla Maestra de Archivos.

UCP: Unidad Central de Procesamiento.

UMC: Unidad Microcontroladora.