

O/U 151  
P 26  
II  
(ej. 2)

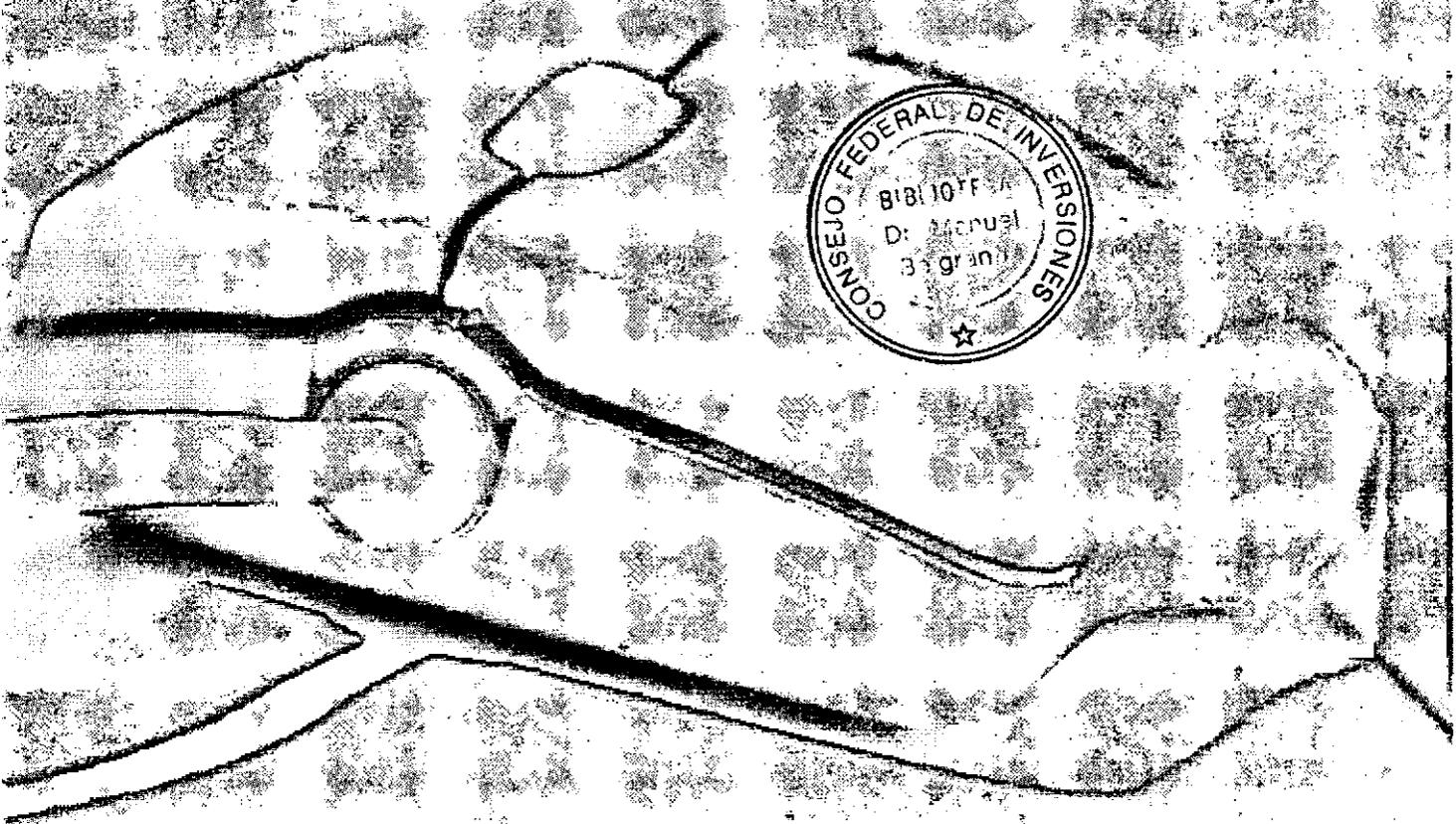
# PROGRAMA

## POLÍTICAS DE SOPORTE PARA LA INTRANET DE GOBIERNO

### AUTOPISTA DE LA INFORMACIÓN

### ADMINISTRACION DEL PARQUE INFORMATICO

### TOMO II



EN LÍNEA

GOBIERNO DE LA PROVINCIA DE SAN LUIS



**INDICE**

**INDICE ..... 1**

**METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I..... 5**

1. PRIMERA ETAPA:..... 5

2. SEGUNDA ETAPA: ..... 5

3. TERCERA ETAPA:..... 6

4. CUARTA ETAPA: ..... 6

5. QUINTA ETAPA:..... 7

6. SISTEMA GUIADO DE PROCESO ..... 8

7. DOCUMENTACIÓN ..... 9

8. AUTORIDAD DE APLICACIÓN Y CONTROL ..... 9

9. FECHA DE REVISIÓN..... 10

10. ANEXO B ..... 11

    Planilla de registraci3n del Inventario de Hardware..... 11

11. ANEXO C ..... 13

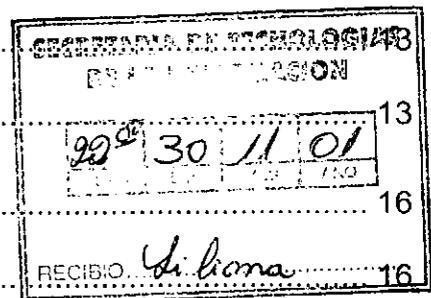
    Planilla de registraci3n del Inventario de Software ..... 13

12. ANEXO D ..... 16

    Modelo de Estampilla para el Inventario Inform3tico ..... 16

**ADMINISTRACI3N DE LICENCIAS ..... 17**

1. PROGRAMA DE ADMINISTRACI3N DE LICENCIAS PARA LA INTRANET  
DE GOBIERNO..... 17



---

<b>ANEXO 1: LEY 25036</b> .....	<b>19</b>
PROPIEDAD INTELECTUAL.....	19
<b>ANEXO 2 "ACUERDOS DE LICENCIAS MICROSOFT"</b> .....	<b>22</b>
1. ACUERDOS DE LICENCIAS MICROSOFT .....	22
2. ACUERDOS DE LICENCIA INDIVIDUAL DEL USUARIO DE MICROSOFT (EULAS).....	23
Derecho legal a usar el programa: .....	23
Copia del programa: Instale uno - no copie ninguno! .....	23
Una computadora - un sistema operativo:.....	24
Revisión de la Licencia de Usuario Final Microsoft .....	24
<b>ANEXO 3: FORMULARIO PARA ACTUALIZACIÓN DE LICENCIAS</b> .....	<b>26</b>
<b>POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS</b> .....	<b>27</b>
1. CONCIENTIZACIÓN DE LOS USUARIOS .....	27
2. FORMAS DE EVITAR LA INFECCIÓN (ANTIVIRUS) .....	27
Identificación .....	29
Técnicas de detección.....	31
Análisis heurístico.....	31
Eliminación .....	32
Comprobación de integridad .....	33
Proteger áreas sensibles.....	35
Demonios de protección.....	37
Aplicar cuarentena.....	38
Definiciones antivirus.....	38

---

3. POLÍTICAS DE PROTECCIÓN .....	39
Conclusión del trabajo .....	44
<b>BIBLIOGRAFÍA.....</b>	<b>45</b>
<b>ANEXO 1.....</b>	<b>46</b>
<b>ADMINISTRACIÓN DE SOFTWARE.....</b>	<b>49</b>
Introducción:.....	49
Objetivo: .....	49
Desarrollo: .....	49
Costos de Software: .....	52
Costos Directos: .....	52
Costos Indirectos:.....	53
Beneficios:.....	53
Reasignación de Programas: .....	54
4. ESTANDARIZACIÓN.....	55
5. CONCLUSIÓN .....	58
<b>PROGRAMA DE MANTENIMIENTO .....</b>	<b>59</b>
1. PROGRAMA DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO.....	59
Sustitución de piezas.....	60
Estado inicial de las máquinas .....	60
Requisitos organizativos a las empresas licitantes.....	61
Requisitos sobre almacenamiento y distribución de repuestos. ....	61
Requisitos sobre confidencialidad de datos almacenados en equipos.....	62
Reparación de equipos.....	62

---

2. ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DEL	
SERVICIO DE MANTENIMIENTO .....	63
Análisis de las necesidades de la APP .....	64
Factores relevantes en el proceso de contratación .....	66
3. CONCLUSIÓN .....	69
<b>SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO .....</b>	<b>70</b>
1. PROGRAMA DESARROLLADO A MEDIDA .....	70
2. MANUAL DE INSTALACIÓN .....	70
Recolección Manual .....	70
Forma Remota.....	75

*METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I.*

---

**METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I.**

1. PRIMERA ETAPA:

Se procede a realizar un inventario físico para lograr el recuento de todas las computadoras de la APP, se debe tener en cuenta en el inventario todas las computadoras (MAC y PC), incluyendo servidores, computadoras portátiles y también toda otra computadora que no se encuentre en uso.

2. SEGUNDA ETAPA:

Se le asigna a cada una de las computadoras un número de serie compuesto por nueve dígitos divididos en cuatro secciones, indicando el primer dígito los niveles que conforman la APP, los tipos de Empresas y Sociedades del Estado. Se tiene un código diferente para la Administración Central, Los Organismos Descentralizados, Las Instituciones de Seguridad Social y cada tipo de empresa y Sociedades del Estado. El Segundo y Tercer Dígito identifican las distintas Jurisdicciones. El cuarto y quinto corresponden a la numeración correlativa de las entidades públicas. El Sexto se reserva para los distintos programas dependientes de las distintas Reparticiones. Los tres restantes en forma consecutiva indicarán los distintos equipos asignados a la repartición. Esta asignación se realiza según la tabla de correspondencias incluida en el Apéndice A. Para identificar unívocamente cada computadora y evitar una doble registración se adhiere a cada máquina relevada una estampilla con el número que le corresponde, cuyo diseño puede apreciarse en el apéndice D. Ej. En la Gerencia de Servicios San Luis, dependiente de la Secretaria de Estado de Tecnologías de la Información, el gabinete de la primera PC inventariada deberá tener el siguiente número:

## METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I.

---

1-10-43-0-001, los primeros seis dígitos nos identifican la dependencia a la que pertenece la PC, mientras que los tres últimos en forma consecutiva indican los distintos gabinetes y sus periféricos inventariados.

### 3. TERCERA ETAPA:

Se procede al relevamiento del Hardware existente, para ello se debe concurrir a cada Repartición y en cada PC, se arranca la misma; si se trata de un "clon" se detiene la máquina en el momento del "booteo" y se anotan los datos de la pantalla de resumen que se observa. En el caso de las computadoras de marca reconocida, usualmente no muestran esta pantalla de resumen y la reemplazan por un logo de la marca, en estos casos se utiliza la información proporcionada por el BIOS, usualmente denominada System Summary, o resumen del sistema. Para acceder a esta información se debe presionar una combinación de teclas durante el arranque de la máquina que se muestra en pantalla, usualmente ctrl. + Alt + Esc, F2, F10 ó Supr. en el cual se observa el registro del Hardware instalado en cada PC de cada repartición lo que se asienta en las planillas correspondientes que se incluyen en el apéndice B.

### 4. CUARTA ETAPA:

Se realiza un inventario del software instalado en todas las computadoras relevadas en el inventario físico, incluyendo aquellas que no se encuentren en uso.

Si bien existen numerosas herramientas de software disponibles en el mercado para asistir en la realización de este proceso, se optó por utilizar un programa diseñado por la BSA ([www.bsa.org](http://www.bsa.org)) denominado SoftScan por cuanto su licencia es Freeware, es decir gratuita y brinda una buena forma de documentar todo el

## METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I.

---

software instalado en una computadora. En el apéndice E se incluye un pequeño manual del manejo básico de este programa. Esta etapa insume mucho tiempo debido al gran tamaño del PI de la APP. Es muy importante asegurarse de que ningún empleado de la APP agregue o quite algún programa durante el tiempo que dure este relevamiento, sin previa comunicación a la Gerencia de Tecnología, lo cual desactualizaría el inventario. Contemplando estos posibles inconvenientes se decidió incluir la posibilidad de actualizar la composición de este inventario, solicitando a cada responsable informático que informe de ABM de inventario a través del correo electrónico o de la Intranet de Gobierno y se prevé la realización de muestreos semestrales en algunas de las Reparticiones elegidas al azar para evitar la desactualización de los datos recabados.

### 5. QUINTA ETAPA:

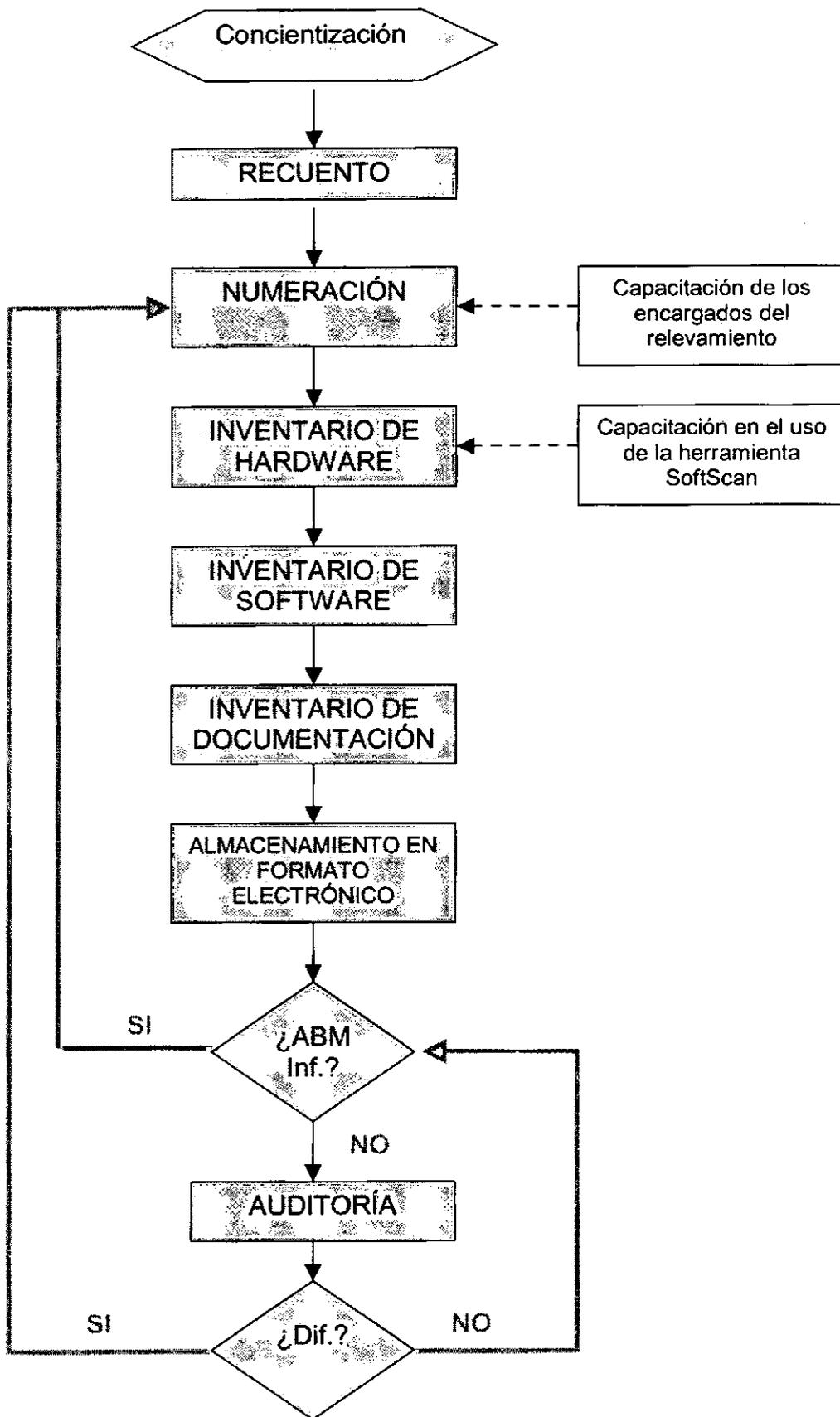
se procede a realizar un inventario *de toda la* documentación del Software instalado en la APP, que debe incluir lo siguiente:

- Todos los disquetes y discos compactos utilizados para instalar el software en las computadoras.
- Todos los manuales de uso y documentación técnica originales.
- Todas las licencias de uso.
- Facturas y otras pruebas de la compra del software, incluyendo las facturas de los equipos de cómputo que fueron entregados con software preinstalado.

La documentación necesaria para registrar el relevamiento del Software instalado en la APP se incluye en el apéndice C.

METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I.

6. SISTEMA GUIADO DE PROCESO



## METODOLOGÍA PARA LA REALIZACIÓN DE UN INVENTARIO DEL P. I.

---

### 7. DOCUMENTACIÓN

Generación de la documentación necesaria para el registro eficiente de los resultados del relevamiento.

Analizando la abundante documentación que se posee de los inventarios realizados en todo el mundo con motivo del problema denominado efecto año 2000, y teniendo en cuenta necesidades y características propias de la APP concluimos en que debemos utilizar una documentación que permita cumplir con dos metas fundamentales:

- Facilidad de registración, tabulación y migración a una base de datos.
- No perder detalles importantes del relevamiento de Hardware y Software.

Para lograr estos ambiciosos objetivos se adopta la documentación incluida en los apéndices, la cual se testeó en diferentes dependencias a modo de prueba piloto y se fue perfeccionando con las sucesivas entrevistas, para lograr una facilidad y rapidez de registración por parte del encargado de realizar el relevamiento, lo que permite conseguir un menor tiempo de entrevista con los referentes informáticos de cada dependencia de la APP.

Una vez concluido el inventario, comenzamos una etapa muy importante, como es la clasificación, tabulación, carga y posterior procesamiento electrónico de los datos recabados para cumplir con esto se utilizan bases de datos creadas a tal fin con la herramienta Microsoft Access del paquete Office 2000.

### 8. AUTORIDAD DE APLICACIÓN Y CONTROL

Se fija como autoridad de aplicación a la Gerencia de Servicio San Luis por ser el organismo más idóneo, en tanto que se le atribuye la función de contralor a la

---

Secretaría de Estado de Tecnologías de la Información, que deberá contar con el asesoramiento del Ministerio de Hacienda y Obras Públicas.

#### 9. FECHA DE REVISIÓN

Esta Metodología estará sujeta a revisión cada tres años, para contemplar posibles cambios tecnológicos o de otra índole que hagan necesario realizar algunos reajustes o cambios.

10. ANEXO B

**Planilla de registraci3n del Inventario de Hardware.**

**MINISTERIO:**  
**REPARTICION:**

Nº de inventario: \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_

	Marca	Modelo	nº serie / nº inventario
CPU			

- Procesador Tipo: \_\_\_\_\_ [ ] MHZ
- Memoria RAM [ ] MB
- Disco R3gido [ ] GB / MB
- Disco R3gido \* [ ] GB / MB
- Diskettera 3 1/2
- Diskettera 5 1/4
- CD - ROM [ ] X
- DVD [ ] X
- Placa de Sonido
- Placa de Red
- Modem Interno
- USB
- Parlantes
- Otro .....

Nº de inventario: \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_

	Marca	Modelo	nº serie / nº inventario	Pulgadas
MONITOR				

Nº de inventario: \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_

	Marca	Modelo	nº serie / nº inventario	Tipo
IMPRESORA				

Nº de inventario: \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_

	Marca	Modelo	nº serie / nº inventario	Tipo
SCANNER				

Nº de inventario: \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_ - \_\_\_

	Marca	Modelo	nº serie / nº inventario	Tipo
TECLADO				

	Marca	Modelo	nº serie / nº inventario	Tipo
MOUSE				
OTRO				

**Instrucciones de Llenado:** Marque con una cruz en el recuadro que corresponda, en Ministerio, coloque el nombre del Ministerio o la Secretaría de estado del cual depende la repartición.

11. ANEXO C

**Planilla de registraci3n del Inventario de Software**

Hoja 1

Gobierno de la Provincia de San Luis  
Secretaria de Tecnologías de la Informaci3n

**Inventario Informático Provincial**

**SOFTWARE**

F-3

Jurisdicci3n	<input type="text"/>	<input type="text"/>
Unidad Ejecutora	<input type="text"/>	<input type="text"/>
Localidad	<input type="text"/>	<input type="text"/>

**SISTEMAS OPERATIVOS Y ENTORNOS**

Ms-Dos	<input type="checkbox"/>	Versi3n	<input type="checkbox"/>	Nro. De Licencia	<input type="text"/>												
Windows	<input type="checkbox"/>	3.1	<input type="checkbox"/>	3.11	<input type="checkbox"/>	95	<input type="checkbox"/>	98	<input type="checkbox"/>	2000	<input type="checkbox"/>	NT.S	<input type="checkbox"/>	NT.WS	<input type="checkbox"/>	Nro. De Licencia	<input type="text"/>
Otro	<input type="text"/>											Nro. De Licencia	<input type="text"/>				

**EDITOR DE TEXTO**

<input type="checkbox"/>										
Word 95	Word 97	Word 2000	Word-dos	Word perfect	Ami-Pro	WordStar	Work	Write	Otro	
Nro. De Licencia										<input type="text"/>

**PLANILLA DE CALCULO**

<input type="checkbox"/>						
Excel 95	Excel97	Excel 2000	Lotus	Works	Quattro	Otro
Nro. De Licencia						<input type="text"/>

Declaro que los datos indicados en la presente son correctos

San Luis, .....

.....  
Firma del Inventariante

.....  
Firma del Responsable  
De la Repartici3n

Hoja 2

Gobierno de la Provincia de San Luis  
Secretaría de Tecnologías de la Información

**SOFTWARE**

F-4

Jurisdicción	<input type="text"/>	<input type="text"/>
Unidad Ejecutora	<input type="text"/>	<input type="text"/>
Localidad	<input type="text"/>	<input type="text"/>

**OTROS SISTEMAS**

Sistema
1
2
3
4
5
6
7
8
9
10
11
12

Declaro que los datos indicados en la presente son correctos

San Luis, .....

.....  
Firma del Inventariante

.....  
Firma del Responsable  
De la Repartición

---

**Instructivo:**

*Descripción de las columnas a completar:*

**Computadora:** Se debe colocar la marca y el tipo de microprocesador (286, 386, 486, pentium, etc.)

**Sistema Operativo:** Indique con una X el sistema operativo que tiene instalado y la versión. En MS-DOS, si no conoce la versión, para conocerla ejecute el comando VER.

**Planilla de Cálculo:** Marque con una X las planillas de cálculo instaladas en la PC.

**Editor de Texto:** Señale con una X los programas instalados en la PC que utiliza como editores de texto.

**Red:** Indique con una X si la computadora a la que hace mención está conectada a alguna red local a través de la placa de red correspondiente.

**Propietario:** Se debe poner el nombre de la repartición propietaria del equipo. Por ejemplo, si el equipo es de otra repartición y está a préstamo en la que se encuentra, deberá indicar el nombre de la repartición de la que depende patrimonialmente la máquina.

**Dudas:**

Por cualquier duda que pueda surgir en el llenado de la planilla o para ampliar información, por favor comunicarse con la Gerencia de Servicios San Luis.

---

**12. ANEXO D****Modelo de Estampilla para el Inventario Informático**

	<b>Inventario de Hardware y Software del Parque Informático Provincial</b>	
Nro. 0-00-00-0-00	Fecha: / /2001	
<ul style="list-style-type: none"><li>• Esta estampilla no debe ser dañada, desprendida, ni adulterada.</li><li>• Ante su deterioro comuníquese con la Secretaría de Estado d Tecnologías de la Información</li></ul>		

Esta estampilla deberá ser adherida a los monitores, Gabinetes, impresoras, teclados y Escáner. Para su identificación durante la realización del inventario de Hardware en cada dependencia, en un lugar visible y no expuesto a roces que podrían dañarla. Es necesario aclarar que el tamaño de la estampilla que se muestra en esta página no se ajusta a la realidad y que la verdadera es de un tamaño menor para facilitar su colocación en el Hardware que corresponda

## **ADMINISTRACIÓN DE LICENCIAS**

### **1. PROGRAMA DE ADMINISTRACIÓN DE LICENCIAS PARA LA INTRANET DE GOBIERNO**

En base al análisis efectuado de la legislación Nacional e Internacional en materia de licenciamiento de software podemos definir los puntos a tener en cuenta en el caso del GPSL para poder administrar las licencias de software adquiridas, optimizando costos y cumpliendo con la ley:

- Designar un Referente Informático por repartición que será el responsable de controlar la cantidad de Licencias que se necesitan en su área para evitar pérdidas y facilitar la actualización del software en caso de ser necesario de manera adecuada aprovechando ofertas de actualizaciones (Upgrades) económicas, usualmente ofrecidas por las principales empresas de Software.
- El referente Informático deberá actualizar mensualmente la adquisición por parte de su área de software, correctamente licenciado, para ello se prevé la colocación de un formulario en la Intranet de Gobierno (incluido el él anexo 3).
- Centralizar la supervisión y control de las licencias correspondientes a todas las reparticiones de la Intranet de Gobierno en la secretaría de Estado de Tecnologías de la Información (SETI).
- Instruir a los administradores de red para que no autoricen la creación de mayor cantidad de usuarios de los que permita la o las licencias correspondientes a cada programa, para evitar el uso excesivo de los mismos por mayor cantidad de usuarios de los cuales estén autorizados.
- Se deben adquirir si están disponibles licencias tipo empresariales (En el caso de ser software de la empresa Microsoft deberán ser Licencias Tipo

## ADMINISTRACIÓN DE LICENCIAS

---

MOLP) que son más económicas por los descuentos que se obtienen al ser una compra de gran volumen y por que sólo se compra un paquete del programa con un juego de manuales y se paga por el permiso de utilizar el mismo en una determinada cantidad de usuarios. Además pueden adquirirse por separado la cantidad de manuales que hagan falta.

- Las compras de software de las distintas reparticiones del GPSL deberán tener la autorización de la SETI. Esto evitará la adquisición de cualquier programa sin licencia y permitirá la estandarización del software a adquirir.
- Se redistribuirán las licencias y los programas que no se utilicen en una repartición a las que lo necesiten evitando de este modo el costo de tener recursos ociosos.

Para efectuar una inversión inteligente en software, la comprensión y el análisis de los Acuerdos de Licencia de todos los programas de software en uso es el punto de partida.

**ANEXO 1: LEY 25036**



Sancionada el 14 de Octubre de 1998 y promulgada en Noviembre de 1998

**PROPIEDAD INTELECTUAL**

Modifícanse los artículos 1º, 4º, 9º y 57 e incorpórase el artículo 55 bis a la Ley N° 11.723

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

**ARTICULO 1º:** - Modifícase el artículo 1º de la ley 11.723, el que quedará redactado de la siguiente manera:

Artículo 1º: A los efectos de la presente ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales; las obras dramáticas, composiciones musicales, dramático-musicales; las cinematográficas, coreográficas y pantomímicas, las obras de dibujo, pintura, escultura, arquitectura; modelos, y obras de arte o ciencias aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas; en fin, toda producción científica, literaria, artística o didáctica, sea cual fuere el procedimiento de reproducción.

La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí.

**ARTICULO 2º:** - Incorpórase como inciso d) del artículo 4º de la ley 11.723 el siguiente texto:

Artículo 4º:...

d) Las personas físicas jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.

**ARTICULO 3º:** - Incorpórase como segundo párrafo del artículo 9º de la Ley 11.723 el siguiente texto:

Artículo 9º:...

Quien haya recibido de los autores o de sus derecho-habientes de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguardia de los ejemplares originales del mismo.

Dicha copia deberá estar debidamente identificada, con indicación del licenciado que realizó la copia y fecha de la misma. La copia de salvaguardia no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.

**ARTICULO 4º:** - Incorpórase como artículo 55 bis de la Ley 11.723 el siguiente texto:

Artículo 55 bis: La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción.

**ARTICULO 5º:** - Incorpórase como artículo 57, in fine, de la ley 11.723 el siguiente texto:

Artículo 57, in fine: Para los programas de computación, consistirá el depósito de los elementos y documentos que determine la reglamentación.

**ARTICULO 6º:** - Comuníquese al Poder Ejecutivo.

---

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS  
AIRES, A LOS CATORCE DIAS DEL MES DE OCTUBRE DEL AÑO MIL  
NOVECIENTOS NOVENTA Y OCHO.

- REGISTRADO BAJO EL N° 25.036.-

ALBERTO PIERRI - CARLOS F. RUCKAUF - Esther H. Pereyra Arandia de Pérez  
Pardo - Mario L. Pontaquarto

Decreto Nro. 1307/98

Bs.As. 6/11/98

POR TANTO:

Téngase por Ley de la Nación N° 25.036 cúmplase, comuníquese, publíquese, dése  
a la Dirección Nacional del Registro Oficial y archívese.

MENEM - Jorge A. Rodriguez - Raúl E. Granillo Ocampo

**ANEXO 2 "ACUERDOS DE LICENCIAS MICROSOFT"**

---

**ANEXO 2 "ACUERDOS DE LICENCIAS MICROSOFT"**

Debido a la importancia a nivel mundial de esta empresa, y a que tiene cautivo a la mayor parte del mercado con sus productos, que se están convirtiendo poco a poco en un estándar de facto, se decide incluir en este anexo un ejemplo concreto de los distintos tipos de acuerdos de licenciamiento, ofrecidos por esta prestigiosa empresa, que fue extraído de su sitio en Internet: [www.microsoft.com](http://www.microsoft.com).

**1. ACUERDOS DE LICENCIAS MICROSOFT**

Los Acuerdos de Licencia varían ampliamente en sus provisiones, posibilidades de descuentos e inclusive en sus nombres. En esta sección, se presentarán y explicarán los Acuerdos de Licencia Microsoft. Esto ayudará a las organizaciones a entender los Acuerdos de Licencia individuales de Microsoft, así como también los Programas de Licencia por Volumen, y ayudarán a acelerar el proceso de adquisición de software y al mismo tiempo reducirán los costos.

Cada producto legítimo Microsoft incluye un Acuerdo de Licencia. El Acuerdo de Licencia individual Microsoft se llama Acuerdo de Licencia de Usuario Final (EULA). Es un contrato entre la persona que adquiere el software y Microsoft.

Adicionalmente al Acuerdo de Licencia individual, Microsoft ofrece Programas de Licenciamiento Por Volumen para empresas y organizaciones. Estos Programas por Volumen ofrecen una variedad de descuentos diferentes, dependiendo de la cantidad de licencias obtenidas. El Programa Microsoft Open License es ideal para empresas con 5 o más PCs, mientras que el Programa de Licencia Select está diseñado para grandes organizaciones con 2.000 o más PCs.

## ANEXO 2 "ACUERDOS DE LICENCIAS MICROSOFT"

---

Para ciertos clientes educacionales, Microsoft ofrece un Programa de Licenciamiento Educacional. Las Instituciones Educacionales y oficinas administrativas o los directorios de Instituciones Educacionales pueden beneficiarse de este programa. Como cualquier otro producto de software, los productos Microsoft están regidos por los EULAs, así también como las leyes de propiedad intelectual de los países específicos donde han sido comprados.

### 2. ACUERDOS DE LICENCIA INDIVIDUAL DEL USUARIO DE MICROSOFT (EULAS)

Al adquirir software Microsoft y abrirlo, la persona acepta los términos del acuerdo de licencia (EULA) y se garantiza el derecho a usar el software. Es importante guardar el EULA en un lugar seguro porque es la prueba de pertenencia legal y le da a su dueño el derecho de usar el programa de software.

Las condiciones más importantes de los EULAs de Microsoft incluyen:

#### **Derecho legal a usar el programa:**

Una licencia garantiza el derecho legal a usar el programa. Una vez que el programa está instalado, está siendo usado. Por lo tanto, una licencia es necesaria cada vez que el software es instalado, se cargue en el disco duro o en la memoria temporal (RAM). Algunos programas pueden garantizar excepciones a la regla mencionada; siempre están detalladas en el EULA.

#### **Copia del programa: Instale uno - no copie ninguno!**

Los programas de software solo pueden ser copiados o duplicados por su productor (por ejemplo Microsoft), salvo que el copiadore tenga la autorización específica del editor del software. Algunos EULAs pueden permitirle hacer copias con el propósito

**ANEXO 2 "ACUERDOS DE LICENCIAS MICROSOFT"**

de la seguridad (una copia de resguardo). Si este es el caso, está establecido en el EULA.

**Una computadora - un sistema operativo:**

Cada computadora o estación de trabajo necesita su propia licencia para el sistema operativo que la opera, inclusive si está siendo instalada sobre la red.

**Revisión de la Licencia de Usuario Final Microsoft**

Aquí hay una revisión de los productos Microsoft más populares y las explicaciones de sus Acuerdos de Licencia.

 <b>Productos de Aplicación</b>	<b>Explicación del EULA</b> (Acuerdo de Licencia de Usuario Final)
Microsoft Office para Windows® 97, Microsoft Word 97, Microsoft Excel 97, PowerPoint® 97, Microsoft Access 97, Works, Publisher 97 y FrontPage 2.0	Está autorizado a instalar Microsoft Office u otros productos de aplicación en una computadora. Puede hacer una segunda copia para su uso exclusivo en una computadora portátil.
 <b>Productos de Sistemas</b>	<b>Explicación del EULA</b>
Sistema Operativo Windows 95	Está autorizado a instalar Windows 95 solo en una computadora.
Sistema Operativo Windows NT® Workstation	Está autorizado a instalar Windows NT Workstation solo en una computadora.
 <b>Productos Multimedia</b>	<b>Explicación del EULA</b>
Productos Multimedia (Encarta® Multimedia Encyclopedia, Cinemania® Interactive Movie Guide, Mozart, Dinosaurs, etc.)	Está autorizado a instalar el CD-ROM del producto Multimedia en una sola computadora.

## ANEXO 2 "ACUERDOS DE LICENCIAS MICROSOFT"

 <b>Productos de Lenguaje</b>	<b>Explicación del EULA</b>
Visual Basic® 4.0 Programming System for Windows	Está autorizado a instalar copias de Visual Basic 4.0 en un número ilimitado de computadoras siempre que Ud. sea el único individuo que use el producto.
Visual C++® 4.0 Programming System for Windows	Está autorizado a instalar Visual C++ en una sola computadora.
 <b>Productos de la familia Back Office</b>	<b>Explicación del EULA</b>
BackOffice 2.0 Server License	Está autorizado a instalar Back Office en un solo servidor.
BackOffice 2.0 Client Access License y Systems Management Server Client Access License	<i>Solo Modo Per Seat</i> : Tiene el derecho para una computadora Cliente particular para acceder a todo el Back Office o componente de software <b>Systems Management Server</b> corriendo en cualquier servidor de la organización. No tiene los derechos de Modo Per Server.
Windows NT Server 3.51, SQL Server 6.5, Microsoft Exchange Server 4.0 y SNA Server 2.11, Licencia de Producto Server	Está autorizado a instalar el producto en un servidor solamente.
Client Access Licenses para Windows NT Server 3.51, SQL Server 6.5, Microsoft Exchange Server 4.0 y SNA Server 2.11	<p><i>Modo Per Seat</i>: Tiene el derecho para un Cliente PC para acceder a todos los Windows NT Server 3.51, SQL Server 6.5, Microsoft Exchange Server 4.0 o SNA Server 2.11 software componente corriendo en cualquier server en la organización. O elija:</p> <p><i>Modo Per Server</i> : Tiene el derecho para un Cliente PC para acceder a un Servidor particular corriendo Windows NT Server 3.51, SQL Server 6.5, Microsoft Exchange Server 4.0 o SNA Server 2.11. Se permite una conexión concurrente adicional a ese servidor.</p>
Microsoft Exchange Connectors. Incluye X.400, Internet Mail y Microsoft Exchange Connectors	Está autorizado a instalar software Microsoft Exchange Server Connector en un solo Servidor.
Microsoft Internet Explorer 3.0	Puede usar Microsoft Internet Explorer solo en conjunto con una copia de licencia válida de Microsoft Windows 95 o Windows NT. Puede bajar y hacer copias del Microsoft Internet Explorer para usar en todas las computadoras para las cuales ha licenciado Windows 95 o Windows NT Workstation.

Esta información no excede ninguna licencia de producto Microsoft. Por favor consultar el acuerdo de licencia que acompaña su producto Microsoft para los términos específicos y condiciones de uso del producto.

**ANEXO 3: FORMULARIO PARA ACTUALIZACIÓN DE LICENCIAS**

**ANEXO 3: FORMULARIO PARA ACTUALIZACIÓN DE LICENCIAS**

Para facilitar la actualización de datos sobre las licencias emitidas a nombre del Gobierno de la Provincia, se incluirá el presente formulario en la Intranet de Gobierno y estará disponible para que los referentes informáticos de cada repartición asienten en él las adquisiciones de software, detallando el tipo de licencia, el número de usuarios que autoriza y la duración del correspondiente contrato de licencia para que la SETI pueda decidir la futura administración de dichas licencias de manera tal de producir un óptimo aprovechamiento de los recursos.

Formulario de Actualización de datos de Licencias de Software						
Ministerio:				Responsable Informático		
Repartición:				.....		
Fecha	Nombre Programa	Fabricante	Nº Licencia	Tipo	Fecha Caducidad	Nº Usuarios Autorizados

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

### POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

#### 1. CONCIENTIZACIÓN DE LOS USUARIOS



Todo proyecto que no posee el apoyo de las personas a las que involucra, no puede salir adelante con facilidad, las trabas impuestas por la típica reacción de los individuos ante nuevas reglas de juego, denominada usualmente "resistencia al Cambio" pueden hacer fracasar un buen proyecto. Teniendo en cuenta esto, se elaboró una campaña de concientización de los usuarios, pretendiendo aclarar el peligro que suponen los virus informáticos y cuales son las medidas que se pueden tomar para minimizar los daños que puedan ocasionar.

#### 2. FORMAS DE EVITAR LA INFECCIÓN (ANTIVIRUS)



Como se menciona en el Manual de Herramientas Informáticas para el Usuario Final (Proyecto 4 "Políticas de Mitigación de Riesgos"), existen dos formas de evitar que los virus dañen el sistema es mediante las copias de respaldo y utilizando antivirus. En el presente trabajo se intenta dar estándares de comportamiento para evitar la infección por virus o evitar que se pierdan datos importantes si es que esta se produce.

Los peligros que implican los virus obligan a que empresas muy importantes se dediquen a buscar la forma de crear programas con fines comerciales que logren combatir los virus que ataquen los sistemas informáticos. Este software es conocido con el nombre de programas antivirus y posee algunas características interesantes para poder cumplir su trabajo.

Como ya dijimos una de las características fundamentales de un virus es propagarse infectando determinados objetos según fue programado. En el caso de los que

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

parasitan archivos, el virus debe poseer algún método para no infectar los archivos con su propio código –para evitar autodestruirse, en otras palabras-, así es que dejan una marca o firma que los identifica de los demás programas o virus.

Para la mayoría de los virus esta marca representa una cadena de caracteres que "inyectan" en el archivo infectado. Los virus más complejos como los polimorfos poseen una firma algorítmica que modificará el cuerpo del mismo con cada infección. Cada vez que estos virus infecten un archivo, mutará su forma y dificultará bastante más las cosas para el software de detección de virus. (Ver Virus polimorfos o mutantes).

El software antivirus es un programa más de computadora y como tal debe ser adecuado para nuestro sistema y debe estar correctamente configurado según los dispositivos de hardware que tengamos. Si trabajamos en un lugar que posee conexión a redes es necesario tener un programa antivirus que tenga la capacidad de detectar virus de redes. Los antivirus reducen sensiblemente los riesgos de infección pero cabe reconocer que no serán eficaces el cien por cien de las veces y su utilización debería estar acompañada de otras formas de prevención, algunas de las cuales se mencionan luego.

La función primordial de un programa antivirus es detectar la presencia de un posible virus para luego poder tomar las medidas necesarias. El hecho de poder erradicarlo podría considerarse como una tarea secundaria ya que con el primer paso habremos logrado frenar el avance del virus, para evitar mayores daños.

Antes de definir en mayor detalle en que consiste el software antivirus es importante que establezcamos claramente la diferencia entre detectar un virus e identificar un virus. El detectar un virus es reconocer la presencia de un accionar virósico en el sistema de acuerdo a las características de los tipos de virus. Identificar un virus es

## ***POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS***

---

poder reconocer qué virus es de entre un montón de otros virus cargados en nuestra base de datos. Al identificarlo sabremos exactamente como actúa, facilitando en consecuencia su posterior eliminación.

De estos dos métodos es importante que un antivirus sea más fuerte en el tema de la detección, ya que con este método podremos encontrar virus todavía no conocido (de reciente aparición) y que seguramente no estarán registrados en nuestra base de datos debido a que su tiempo de dispersión no es suficiente como para que hayan sido analizados por un grupo de expertos de la empresa del antivirus.

### **Identificación**



Identificar un virus supone, primero, lograr su detección y luego poder determinar de qué virus se trata exactamente. A esta técnica se la conoce con el nombre de escaneo. Funciona de la siguiente manera:

El programa antivirus posee una base de datos con ciertas strings (cadenas) propias de cada virus. Estas strings no son más que las firmas que mencionamos más atrás en el texto, o sea cadenas de caracteres que el scanner del antivirus utilizará como huella digital para identificar de qué virus se trata. El scanner comienza a revisar uno por uno el código de los archivos almacenados intentando encontrar alguno de estos fragmentos representativos de los virus que tiene registrados. Con cada una de las verificaciones no se revisa la base de datos completa ya que resultaría bastante trabajoso y en una pérdida de tiempo considerable, aunque de hecho el hacer un escaneo de nuestra unidad de disco rígido lleva algún tiempo. Entonces, cada antivirus utilizará diferentes técnicas algorítmicas para agilizar un poco este paso de comparar el código contra su base de datos.

## *POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS*

---

Actualmente la producción de virus se ve masificada e Internet colabora enormemente en la dispersión de virus de muchos tipos. Muchos de estos virus son creados por usuarios inexpertos con pocos conocimientos de programación y, en muchos casos, por simples usuarios que bajan de Internet programas que crean virus genéricos. Ante tantos "desarrolladores" al servicio de la producción de virus la técnica de scanning se ve altamente superada. Las empresas antivirus están constantemente trabajando en la búsqueda y documentación de cada nuevo virus que aparece. Muchas de estas empresas actualizan sus bases de datos todos los meses, otras lo hacen quincenalmente, y algunas pocas llegan a hacerlo todas las semanas.

La debilidad de la técnica de scanning es inherente al modelo. Debido a que un virus debería alcanzar una dispersión adecuada para que algún usuario lo capture y lo envíe a un grupo de especialistas en virus que luego se encargarán de determinar que parte del código será representativa para ese virus y finalmente lo incluirán en la base de datos del antivirus. Todo este proceso puede llevar varias semanas, tiempo suficiente para que un virus eficaz haga de las suyas. En la actualidad, Internet proporciona el canal de bajada de las definiciones antivirus que nos permitirán identificar decenas de miles de virus que andan acechando. Estas decenas de miles de virus, como dijimos, también influirán en el tamaño de la base de datos.

La técnica de scanning no resulta ser la solución definitiva, ni tampoco la más eficiente, pero continúa siendo la más utilizada debido a que permite identificar con cierta rapidez los virus más conocidos, que en definitiva son los que lograron adquirir mayor dispersión.

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

---

### Técnicas de detección

Teniendo en cuenta los puntos débiles de la técnica de scanning surgió la necesidad de incorporar otros métodos que complementaran al primero. Como ya se mencionó la detección consiste en reconocer el accionar de un virus por los conocimientos sobre comportamiento que se tienen sobre ellos, sin importar demasiado su identificación exacta. Este otro método buscará código que intente modificar la información de áreas sensibles del sistema sobre las cuales el usuario convencional no tiene control –y a veces ni siquiera tiene conocimiento-, como el master boot record, el boot sector, la FAT, entre las más conocidas.

Otra forma de detección que podemos mencionar adopta, más bien, una posición de vigilancia constante y pasiva. Esta, monitorea cada una de las actividades que se realizan intentando determinar cuándo una de éstas intenta modificar sectores críticos de las unidades de almacenamiento, entre otros. A esta técnica se la conoce como chequeo de integridad.

### Análisis heurístico



La técnica de detección más común es la de análisis heurístico.

Consiste en buscar en el código de cada uno de los archivos cualquier instrucción que sea potencialmente dañina, acción típica de los virus informáticos. Es una solución interesante tanto para

virus conocidos como para los que no los son. El inconveniente es que muchas veces se nos presentarán falsas alarmas (cosas que el análisis heurístico considera peligrosas y que en realidad no lo son).

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

---

### Eliminación



La eliminación de un virus implica extraer el código del archivo infectado y reparar de la mejor manera el daño causado en este. A pesar de que los programas antivirus pueden detectar miles de virus, no siempre pueden erradicar la misma cantidad, por lo general pueden quitar los virus conocidos y más difundidos de los cuales pudo realizarse un análisis profundo de su código y de su comportamiento. Resulta lógico entonces que muchos antivirus tengan problemas en la detección y erradicación de virus de comportamiento complejo, como el caso de los polimorfos, que utilizan métodos de encriptación para mantenerse indetectables. En muchos casos el procedimiento de eliminación puede resultar peligroso para la integridad de los archivos infectados, ya que si el virus no está debidamente identificado las técnicas de erradicación no serán las adecuadas para el tipo de virus.

Para muchos el procedimiento correcto consiste en eliminar completamente el archivo y restaurarlo de la copia de respaldo (de allí la importancia de tener una copia de seguridad actualizada). Si en vez de archivos la infección se realizó en algún sector crítico de la unidad de disco rígido la solución es simple, se recomienda particionar nuevamente la unidad y formatearla para asegurarse de la desaparición total del virus, cosa que resultaría poco operativa y fatal para la información del sistema. Como alternativa a esto existe para el sistema operativo MS-DOS / Windows una opción no documentada del comando FDISK que resuelve todo en cuestión de segundos. El parámetro /MBR se encarga de restaurar el registro maestro de booteo (lugar donde suelen situarse los virus) impidiendo así que este vuelva a cargarse en el inicio del sistema. Vale aclarar que cualquier dato que haya en ese sector será sobrescrito y puede afectar a sistemas que tengan la opción de

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

---

bootear con diferentes sistemas operativos. Muchos de estos programas que permiten hacer la elección del sistema operativo se sitúan en esta área y por consiguiente su código será eliminado cuando se usa el parámetro mencionado.

Para el caso de la eliminación de un virus es muy importante que el antivirus cuente con soporte técnico local, que sus definiciones sean actualizadas periódicamente y que el servicio técnico sea apto para poder responder a cualquier contingencia que nos surja en el camino.

### **Comprobación de integridad**

Se verifica que algunos sectores "sensibles" del sistema no sean alterados sin el consentimiento del usuario. Estas comprobaciones pueden aplicarse tanto a archivos como al sector de arranque de las unidades de almacenamiento.

Para poder realizar las comprobaciones el antivirus, primero, debe tener una imagen del contenido de la unidad de almacenamiento desinfectada con la cual poder hacer después las comparaciones. Se crea entonces un registro con las características de los archivos: nombre, tamaño, fecha de creación o modificación y, lo más importante para el caso, el checksum, que es el resultado de aplicar un algoritmo al código del archivo para obtener un valor que será único según su contenido. Si un virus inyectara parte de su código en el archivo la nueva comprobación del checksum sería distinta a la que se guardó en el registro y el antivirus alertaría de la modificación. En el caso del sector de booteo el registro puede ser algo diferente. Como existe un MBR por unidad física y un BR por cada unidad lógica, algunos antivirus pueden guardarse directamente una copia de cada uno de ellos en un archivo y luego compararlos contra los que se encuentran en las posiciones originales.

## *POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS*

---

Una vez que el antivirus conforma un registro de cada uno de los archivos en la unidad podrá realizar las comprobaciones de integridad. Cuando el comprobador es puesto en funcionamiento cada uno de los archivos serán escaneados. Nuevamente se aplica la función checksum y se obtiene un valor que es comparado contra el que se guardó en el registro. Si ambos valores son iguales el archivo no sufrió modificaciones durante el período comprendido entre el registro de checksum antiguo y la comprobación reciente. Por el otro lado, si los valores checksum no concuerdan significa que el archivo fue alterado y en ciertos casos el antivirus pregunta al usuario si quiere restaurar las modificaciones. Lo más indicado en estos casos sería que un usuario con conocimientos sobre su sistema avale que se trata realmente de una modificación no autorizada –y por lo tanto atribuible a un virus-, elimine el archivo y lo restaure desde la copia de respaldo.

La comprobación de integridad en los sectores de booteo no es muy diferente. El comprobador verificará que la copia que está en uso sea igual a la que fue guardada con anterioridad. Si se detectara una modificación en cualquiera de estos sectores, se preguntará al usuario por la posibilidad de reconstruirlos utilizando las copias guardadas. Teniendo en cuenta que este sector en especial es un punto muy vulnerable a la entrada de los virus multipartitos, los antivirus verifican constantemente que no se hagan modificaciones. Cuando se detecta una operación de escritura en uno de los sectores de arranque, el programa antivirus muestra en pantalla un mensaje para el usuario indicándole lo que está por suceder. Por lo general el programa antivirus ofrece algunas opciones sobre como proceder:

- Evitar la modificación
- Dejarla continuar
- Bloquear el sistema

## ***POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS***

---

- No tomar ninguna medida (cancelar).

Para que esta técnica sea efectiva cada uno de los archivos deberá poseer su entrada correspondiente en el registro de comprobaciones. Si nuevos programas se están instalando o estamos bajando algunos archivos desde Internet, o algún otro archivo ingresa por cualquier otro dispositivo de entrada, después sería razonable que registremos el checksum con el comprobador del antivirus. Incluso, algunos de estos programas no dejarán que ningún archivo que no esté registrado corra en el sistema.

### **Proteger áreas sensibles**

Muchos virus tienen la capacidad de "parasitar" archivos ejecutables. Con esto queremos decir que el virus localizará los puntos de entrada de cualquier archivo que sea ejecutable (los archivos de datos no se ejecutan por lo tanto no son utilizados por los virus) y los desviará a su propio código de ejecución. Así, el flujo de ejecución correrá primero el código del virus y luego el del programa y, como todos los virus poseen un tamaño muy reducido para no llamar la atención, el usuario seguramente no notará la diferencia. Esto le permitirá situarse en memoria y empezar a ejecutar sus instrucciones dañinas.

Una vez que el virus se encuentra en memoria puede replicarse a sí mismo en cualquier otro archivo ejecutable. El archivo ejecutable por excelencia que atacan los virus es el COMMAND.COM, uno de los archivos fundamentales para el arranque en el sistema operativo MS-DOS. Este archivo es el intérprete de comandos del sistema, por lo tanto, se cargará cada vez que se necesite la shell. La primera vez será en el inicio del sistema y, durante el funcionamiento, se llamará al COMMAND.COM cada vez que se salga de un programa y vuelva a necesitarse la

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

intervención de la shell. Con un usuario desatento, el virus logrará replicarse varias veces antes de que empiecen a notarse síntomas extraños en la PC.

El otro "ente" ejecutable capaz de ser infectado es el sector de arranque de los discos magnéticos. Aunque este sector no es un archivo en sí, contiene rutinas que el sistema operativo ejecuta cada vez que arranca el sistema desde esa unidad, resultando este un excelente medio para que el virus se propague de una computadora a la otra. Como dijimos antes una de las claves de un virus es lograr permanecer oculto dejando que la entidad ejecutable que fue solicitada por el usuario corra libremente después de que él mismo se halla ejecutado. Cuando un virus intenta replicarse a un disquete, primero deberá copiar el sector de arranque a otra porción del disco y recién entonces copiar su código en el lugar donde debería estar el sector de arranque.

Durante el arranque de la computadora con el disquete inserto en la disquetera, el sistema operativo MS-DOS intentará ejecutar el código contenido en el sector de booteo del disquete. El problema es que en esa posición se encontrará el código del virus, que se ejecuta primero y luego apuntará el puntero de ejecución a la nueva posición en donde se encuentran los archivos para el arranque. El virus no levanta sospechas de su existencia más allá de que existan o no archivos de arranque en el sector de booteo.

Nuestro virus se encuentra ahora en memoria y no tendrá problemas en replicarse a la unidad de disco rígido cuando se intente bootear desde esta. Hasta que su módulo de ataque se ejecute según fue programado, el virus intentará permanecer oculto y continuará replicándose en archivos y sectores de booteo de otros disquetes que se vayan utilizando, aumentando potencialmente la dispersión del virus cuando los disquetes sean llevados a otras máquinas.

### **Demonios de protección**

Consisten en módulos del programa antivirus residentes en memoria que se encargan de impedir la entrada del cualquier virus y verifican constantemente operaciones que intenten realizar modificaciones por métodos poco frecuentes. Estos, se activan al arrancar la computadora y por lo general es importante que se carguen al comienzo y antes que cualquier otro programa para darle poco tiempo de ejecución a los virus y detectarlos antes que alteren algún dato. Según como esté configurado el antivirus, el demonio (como se los conoce en el ambiente Unix) o TSR (en la jerga MS-DOS / Windows), estará pendiente de cada operación de copiado, pegado o cuando se abran archivos, verificará cada archivo nuevo que es creado y todos los downloads de Internet, también hará lo mismo con las operaciones que intenten realizar un formateo de bajo nivel en la unidad de disco rígido y, por supuesto, protegerá los sectores de arranque de modificaciones.

Las nuevas computadoras que aparecieron con formato ATX poseen un tipo de memoria llamada Flash-ROM con una tecnología capaz de permitir la actualización del BIOS de la computadora por medio de software sin la necesidad de conocimientos técnicos por parte del usuario y sin tener que tocar en ningún momento cualquiera de los dispositivos de hardware. Esta nueva tecnología añade otro punto a favor de los virus ya que ahora estos podrán copiarse a esta zona de memoria dejando completamente indefensos a muchos antivirus antiguos. Un virus programado con técnicas avanzadas y que haga uso de esta nueva ventaja es muy probable que sea inmune al reparticionado o reformato de las unidades de discos magnéticos.

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

---

### **Aplicar cuarentena**

Es muy posible que un programa antivirus muchas veces quede descolocado frente al ataque de virus nuevos. Para esto incluye esta opción que no consiste en ningún método de avanzada sino simplemente en aislar el archivo infectado. Antes que esto el antivirus reconoce el accionar de un posible virus y presenta un cuadro de diálogo informándonos. Además de las opciones clásicas de eliminar el virus, aparece ahora la opción de ponerlo en cuarentena. Este procedimiento encripta el archivo y lo almacena en un directorio hijo del directorio donde se encuentra el antivirus.

De esta manera se está impidiendo que ese archivo pueda volver a ser utilizado y que continúe la dispersión del virus. Como acciones adicionales el antivirus nos permitirá restaurar este archivo a su posición original como si nada hubiese pasado o nos permitirá enviarlo a un centro de investigación donde especialistas en el tema podrán analizarlo y determinar si se trata de un virus nuevo, en cuyo caso su código distintivo será incluido en las definiciones de virus.

### **Definiciones antivirus**



Los archivos de definiciones antivirus son fundamentales para que el método de identificación sea efectivo. Los virus que alcanzaron una considerable dispersión pueden llegar a ser analizados por los ingenieros especialistas en virus de algunas de las compañías antivirus, que mantendrán actualizadas las definiciones permitiendo así que las medidas de protección avancen casi al mismo paso en que lo hacen los virus.

Un antivirus que esté desactualizado puede resultar poco útil en sistemas que corren el riesgo de recibir ataques de virus nuevos (como organismos gubernamentales), y están reduciendo en un porcentaje bastante alto la posibilidad de protección. La

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

---

actualización también puede venir por dos lados: actualizar el programa completo o actualizar las definiciones antivirus. Si contamos con un antivirus que posea técnicas de detección avanzadas, posibilidad de análisis heurístico, protección residente en memoria de cualquiera de las partes sensibles de una unidad de almacenamiento, verificador de integridad, etc., estaremos bien protegidos para empezar. Una actualización del programa sería realmente justificable en caso de que incorpore algún nuevo método que realmente influye en la erradicación contra los virus. Sería importante también analizar el impacto económico, ya que sería totalmente inútil tener el mejor antivirus y preocuparse por actualizar sus definiciones día por medio si nuestra red ni siquiera tiene acceso a Internet, tampoco acceso remoto de usuarios y el único intercambio de información es entre empleados que trabajan con un paquete de aplicaciones de oficina sin ningún contenido de macros o programación que de lugar a posibles infecciones.

### 3. POLÍTICAS DE PROTECCIÓN



En la problemática que nos ocupa, poseer un antivirus y saber cómo utilizarlo es la primer medida que debe tomarse. Pero no será totalmente efectiva si no va acompañada por conductas que el usuario debe respetar. La educación y la información son el mejor método para protegerse.

Un virus informático es un programa de computadora que posee ciertas características que lo diferencian de un programa común, y se infiltra en las computadoras de forma furtiva y sin ninguna autorización. Como cualquier otro programa necesitará un medio físico para transmitirse, por lo tanto los medios utilizados para el transporte de nuestra información resultan un excelente medio

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

aprovechable por los virus. Cualquier puerta que nosotros utilicemos para comunicarnos es una posible vía de ingreso de virus, ya sea una disquetera, una lectora de CD-ROM, un módem con conexión a Internet, la placa que nos conecta a la red de la empresa, los nuevos puertos ultrarrápidos (USB y FireWire) que nos permiten conectar dispositivos de almacenamiento externos como unidades Zip, Jazz, HDDs, etc.

Viendo que un virus puede atacar nuestro sistema desde cualquier ángulo, no podríamos dejar de utilizar estos dispositivos solo porque sean una vía de entrada de virus (ya que para lograr seguridad total deberíamos dejar de utilizarlos a todos, quedando aislados), cualquiera de las soluciones que planteemos no será cien por cien efectiva pero contribuirá enormemente en la protección y estando bien informados evitaremos crear pánico en una situación de infección.

Una manera adecuada de comprobar la infección en un archivo ejecutable es mediante la verificación de integridad. Con esta técnica estaremos seguros de que cualquier intento de modificación del código de un archivo será evitado o, en última instancia, sabremos que fue modificado y podremos tomar alguna medida al respecto (como eliminar el archivo y restaurarlo desde la copia de respaldo). Es importante la frecuencia con la que se revise la integridad de los archivos. Para un sistema grande como el del Gobierno de la Provincia con acceso a redes externas es conveniente una verificación semanal por parte de cada uno de los usuarios en sus computadoras. Un router no tiene manera de determinar si un virus está ingresando a la red de la empresa porque los paquetes individuales no son suficiente cómo para detectar a un virus. En el caso de un archivo que se baja de Internet, éste deberá almacenarse y verificarse con la técnica de scanning, recién entonces habrá que determinar si es un archivo apto para utilizarlo.

## *POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS*

---

En cuanto a los virus multipartitos estaremos cubiertos si tomamos especial cuidado del uso de los disquetes. Estos no deben dejarse jamás en la disquetera cuando no se los está usando y menos aún durante el arranque de la máquina. Una medida acertada es modificar la secuencia de booteo modificando el BIOS desde el programa Setup para que se intente arrancar primero desde la unidad de disco rígido y en su defecto desde la disquetera. Los discos de arranque del sistema deben crearse en máquinas en las que sabemos que están libres de virus y deben estar protegidos por la muesca de sólo lectura.

El programa antivirus debe ser adecuado para el sistema, en nuestro caso elegimos el InoculateIT (Ver Anexo 1). Debe proveer análisis heurístico y debe tener la capacidad de chequear la integridad de sus propios archivos como método de defensa contra los retrovirus. Es muy importante cómo el antivirus guarda el archivo de definiciones de virus. Debe estar protegido contra sobre escrituras, encriptado para que no se conozca su contenido y oculto en el directorio (o en su defecto estar fragmentado y cambiar periódicamente su nombre). Esto es para que los virus no reconozcan con certeza cuál es el archivo de definiciones y dejen imposibilitado al programa antivirus de identificar con quien está tratando.

Regularmente deberemos iniciar la máquina con un disquete "libre de virus" de arranque del sistema operativo y escanear las unidades de disco rígido con unos disquetes que contengan el programa antivirus. Si este programa es demasiado extenso podemos correrlo desde la lectora de CD-ROM, siempre y cuando la hayamos configurado previamente. Las nuevas máquinas de factor ATX incluso nos permiten bootear desde una lectora de CD-ROM, que no tendrán problemas en reconocer ya que la mayoría traen sus drivers en firmware. Si no se cuenta con alguna de estas nuevas tecnologías simplemente podemos utilizar un disco de inicio

## POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS

que nos da la posibilidad de habilitar la utilización de la lectora para luego poder utilizarla con una letra de unidad convencional.

El módulo residente en memoria del antivirus es fundamental para la protección de virus que están intentando entrar en nuestro sistema. Debe ser apto para nuestro tipo de sistema operativo y también debe estar correctamente configurado. Los antivirus actuales poseen muchas opciones configurables en las que deberá fijarse el residente. Cabe recordar que mientras más de estas seleccionemos la performance del sistema se verá mayormente afectada. Adoptar una política de seguridad adecuada implica lograr un equilibrio entre verificar absolutamente todo y lograr velocidad en los trabajos que realicemos.

Se debe mantener actualizada la copia de respaldo del sistema.

No se deben instalar programas que no sean originales o que no cuenten con su correspondiente licencia de uso.

Los archivos con los que trabajen los empleados deberán ser verificados, por un antivirus actualizado, y debe evitarse en lo posible el intercambio de discos entre computadoras del hogar y del Gobierno.

Los programas freeware, shareware, trial, o de cualquier otro tipo de distribución que sean bajados de Internet deberán ser escaneados antes de su ejecución. El download deberá ser sólo de sitios en los que se confía. La autorización de instalación de programas deberá ser requerida al responsable informático de cada área.

Cualquier programa de fuente desconocida que el usuario quiera instalar debe ser correctamente revisado. Si un grupo de usuarios trabaja con una utilidad que no está instalada en la oficina, el responsable informático del área deberá determinar si instala esa aplicación en el servidor y les da acceso a ese grupo de usuarios,

**POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS**

siempre y cuando el programa no signifique un riesgo para la seguridad del sistema.

Nunca debería priorizarse lo que el usuario quiere frente a lo que el sistema necesita para mantenerse seguro.

Todas las computadoras deben tener el par ID de usuario y contraseña.

Nunca se debe dejar disquetes en la disquetera durante el encendido de la computadora. Tampoco utilizar disquetes de fuentes no confiables o los que no halla creado uno mismo.

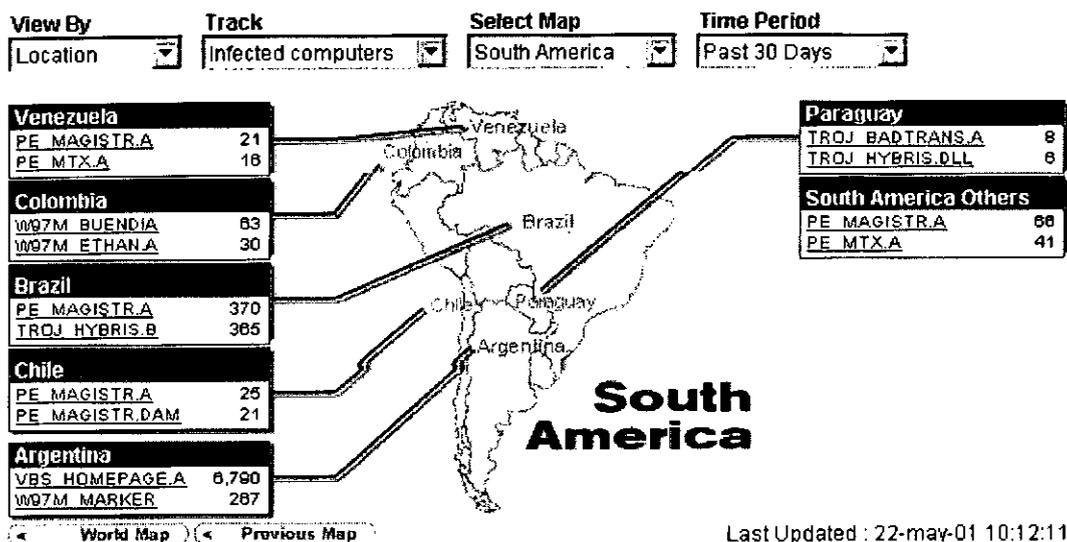
Cada disquete que se valla a utilizar debe pasar primero por un detector de virus.

Con escanear los archivos ejecutables y los que posean macros será suficiente.

Escanear todos los archivos, por lo general, resulta una pérdida de tiempo.

Si el disquete no lo usaremos para grabar información, deberemos protegerlo contra escritura activando la muesca de protección. La protección de escritura estará activada cuando al intentar ver el disco a tras luz veamos dos pequeños orificios cuadrados en la parte inferior.

A continuación se muestra una estadística de la cantidad de virus reportados en América del Sur. Fuente: [www.antivirus.com](http://www.antivirus.com)



## ***POLÍTICAS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS***

---

Cabe aclarar que no todas las infecciones son reportadas pero de cualquier forma es un dato útil.

### **Conclusión del trabajo**

Los virus informáticos no son un simple riesgo de seguridad. Existen miles de programadores en el mundo que se dedican a esta actividad con motivaciones propias y diversas que provocan millones de dólares al año en gastos de seguridad para las empresas. El verdadero peligro de los virus es su forma de ataque indiscriminado contra cualquier sistema informático, cosa que resulta realmente crítica en entornos donde máquinas y humanos interactúan directamente.

Es muy difícil prever la propagación de los virus y que máquina intentarán infectar, de ahí la importancia de saber cómo funcionan típicamente y tener en cuenta los métodos de protección adecuados para evitarlos.

A medida que las tecnologías evolucionan van apareciendo nuevos estándares y acuerdos entre compañías que pretenden compatibilizar los distintos productos en el mercado. Como ejemplo podemos nombrar la incorporación de Visual Basic para Aplicaciones en el paquete Office y en muchos otros nuevos programas de empresas como AutoCAD, Corel, Adobe. Con el tiempo esto permitirá que con algunas modificaciones de código un virus pueda servir para cualquiera de los demás programas, incrementando aún más los potenciales focos de infección.

La forma de que los daños no sean irreparables pasa por tener una conducta previsor, manteniendo las copias de seguridad al día, y tratando de que todo archivo que ingrese a la red provenga de una fuente segura, una buena medida es revisarlos con un antivirus actualizado antes de utilizarlos.

**BIBLIOGRAFÍA**

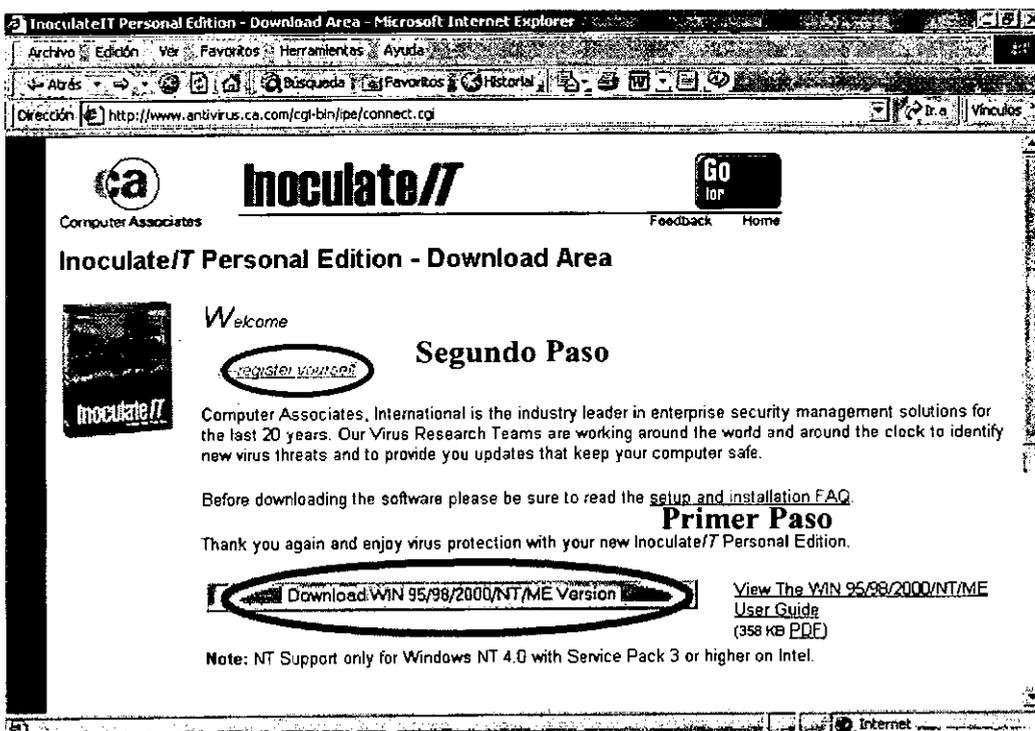
- Virus, Manual de Referencia. Autor, Pedro Luis Córtez, Editorial Metodos
- [www.antivirus.ca.com](http://www.antivirus.ca.com)
- [www.antivirus.com.ar](http://www.antivirus.com.ar)
- [www.symantec.dk/region/mx/avcenter/education](http://www.symantec.dk/region/mx/avcenter/education)
- [www.itacom.com.py/antivirus/virus.html](http://www.itacom.com.py/antivirus/virus.html)
- [www.hispasec.com/](http://www.hispasec.com/)
- [www.pandaantivirus.com.ar/info\\_prevenir\\_el\\_caos.htm](http://www.pandaantivirus.com.ar/info_prevenir_el_caos.htm)
- [www.antivirus.com/vinfo/virusencyclo/default5.asp](http://www.antivirus.com/vinfo/virusencyclo/default5.asp)
- [www.map.es](http://www.map.es)
- [www.sophos.com](http://www.sophos.com)
- [www.pandasoftware.es/enciclopedia](http://www.pandasoftware.es/enciclopedia)
- [www.f-secure.com](http://www.f-secure.com)
- [www.mcafee.com](http://www.mcafee.com)
- [www.commandcom.com](http://www.commandcom.com)

**ANEXO 1**

Luego del análisis de varias opciones en cuanto a programas antivirus se optó por la utilización de una herramienta asequible a cualquier usuario de la Intranet de Gobierno, actualizable, y como la mayoría de los virus que en la actualidad afectan a los sistemas informáticos son del tipo Macro virus, el indicado fue el Inoculate IT.

Se puede obtener una copia de dicho antivirus en el siguiente sitio de Internet: [www.antivirus.ca.com](http://www.antivirus.ca.com).

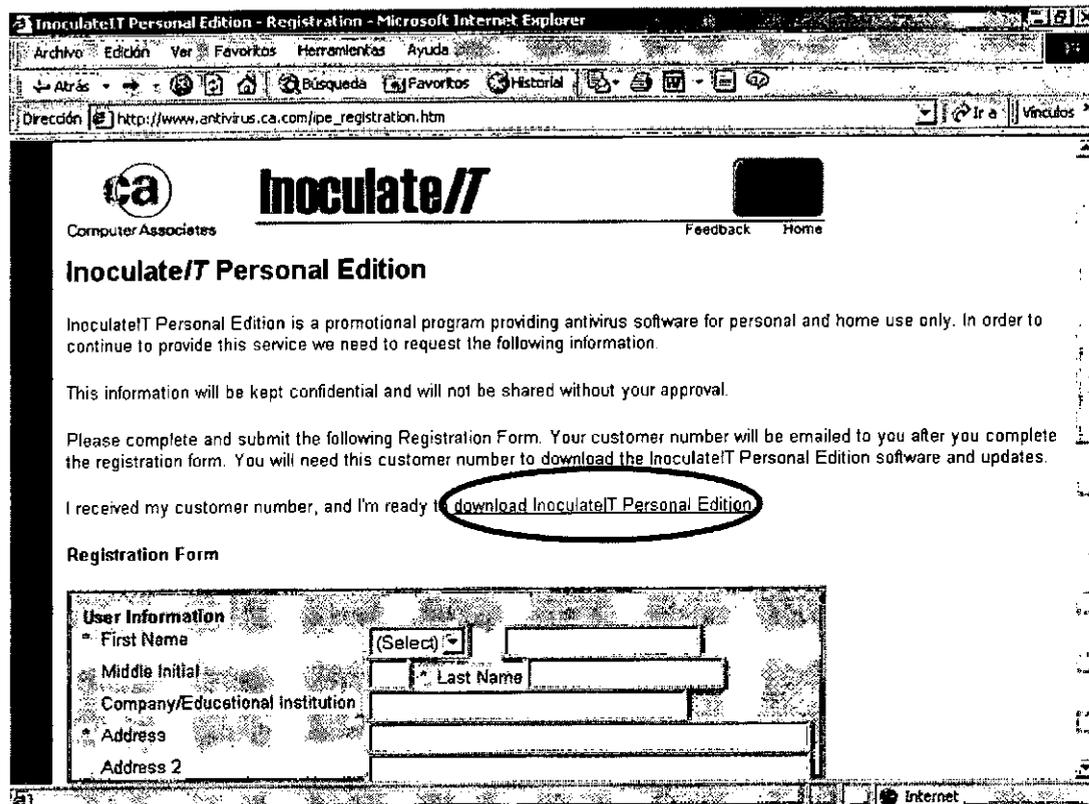
Para efectuar la instalación y la descarga del antivirus se debe ingresar al sitio y elegir la opción Download Win95/98/2000/NT/ME Versión.



Luego de esto se deberá completar una pantalla de registro en la cual se solicitan algunos datos personales del usuario, y una dirección de correo electrónico válida, a la cual se enviará el número de registro del programa. (Primer Paso)

Luego de unas horas se recibirá en el correo electrónico ingresado el código necesario para instalar el programa. Con dicho código se deberá ingresar en la citada página ([www.antivirus.ca.com](http://www.antivirus.ca.com)). Y hacer clic en Paso 2.

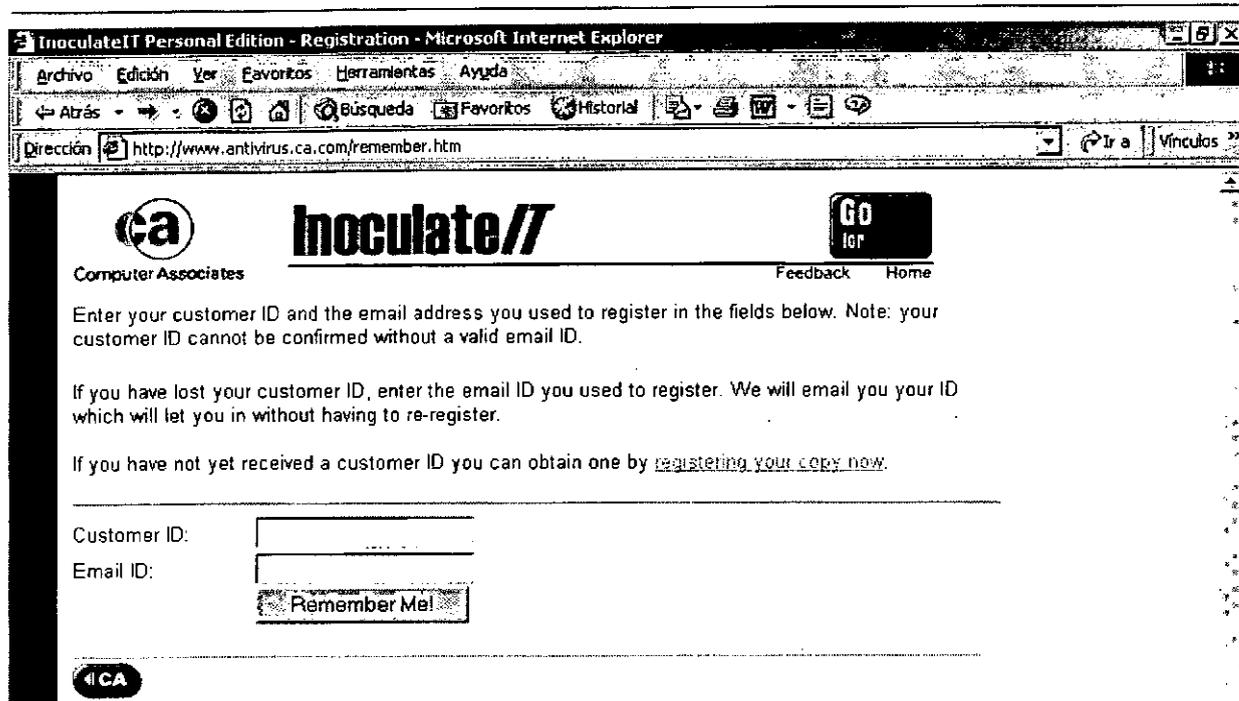
Luego de esto aparecerá la misma pantalla que se utilizó para obtener el número de registro.



En este caso haremos clic en el enlace marcado con el círculo.

Se abrirá a continuación la pantalla en la que nos solicita nuevamente el número de registración, y la dirección de correo nuevamente.

A continuación deberemos ingresar el número de identificación y una dirección de correo electrónico.



Con esto estaremos en condiciones de bajar el archivo ejecutable para instalar el antivirus correctamente.

El asistente de la instalación nos guiará paso a paso durante la instalación.

## **ADMINISTRACIÓN DE SOFTWARE**

### **Introducción:**

Todo proceso de administración debe cumplir con los siguientes pasos:

- Planear
- Organizar
- Analizar
- Medir y
- Controlar

Estos pasos tienden a balancear los costos y generar un ambiente más predecible en el cual las inversiones en software, sean controladas, para optimizar costos en adquisición y mantenimiento de todos los elementos de software.

### **Objetivo:**

Estandarizar la adquisición de software a ser utilizado en el ámbito de la administración Pública Provincial (APP), su mantenimiento y administración; de manera tal de procurar reducir los costos inherentes al mismo.

### **Desarrollo:**

Antes de comprar un determinado paquete de software se deben tener en cuenta una serie de puntos, los cuales deberán ser analizados cuidadosamente para establecer la verdadera necesidad del mismo, y si los costos asociados, se justifican o no:

- Frecuencia estimada de uso
- Importancia del mismo

## ADMINISTRACIÓN DE SOFTWARE

---

- o Cantidad de usuarios previstos
- o Costo de adquisición del paquete de software
- o Costo de las licencias necesarias para utilizar el paquete
- o Costo de futuras actualizaciones o modificaciones
- o Costo de soporte.

**Frecuencia estimada de Uso:** Suele ser un importante indicador de la verdadera necesidad de contar con determinada herramienta, y un respaldo a la hora de justificar la compra de la misma. En la mayoría de los casos, a mayor frecuencia estimada de uso mayor importancia de la herramienta.

**Importancia del Mismo:** Puede medirse, en principio, por su frecuencia estimada de uso, pero es importante aclarar, que dicha frecuencia no es el único indicador que determinará, la importancia de contar, con él, otros indicadores a utilizar son: Beneficios de la utilización de la herramienta a adquirir, Costos asociados con la no adquisición de la misma, etc. Es útil normalmente responder a la pregunta ¿Cuánto pierde y cuanto puede ganar la APP por no contar con la herramienta considerada?. En la respuesta a esta sencilla pregunta, se encontrará un importante indicio a la hora de determinar el grado de importancia del programa en cuestión.

**Cantidad de Usuarios Prevista:** Es un indicador para determinar a priori la cantidad de personal a capacitar en la utilización de la herramienta en cuestión, con los posibles costos de dicha capacitación.

## ADMINISTRACIÓN DE SOFTWARE

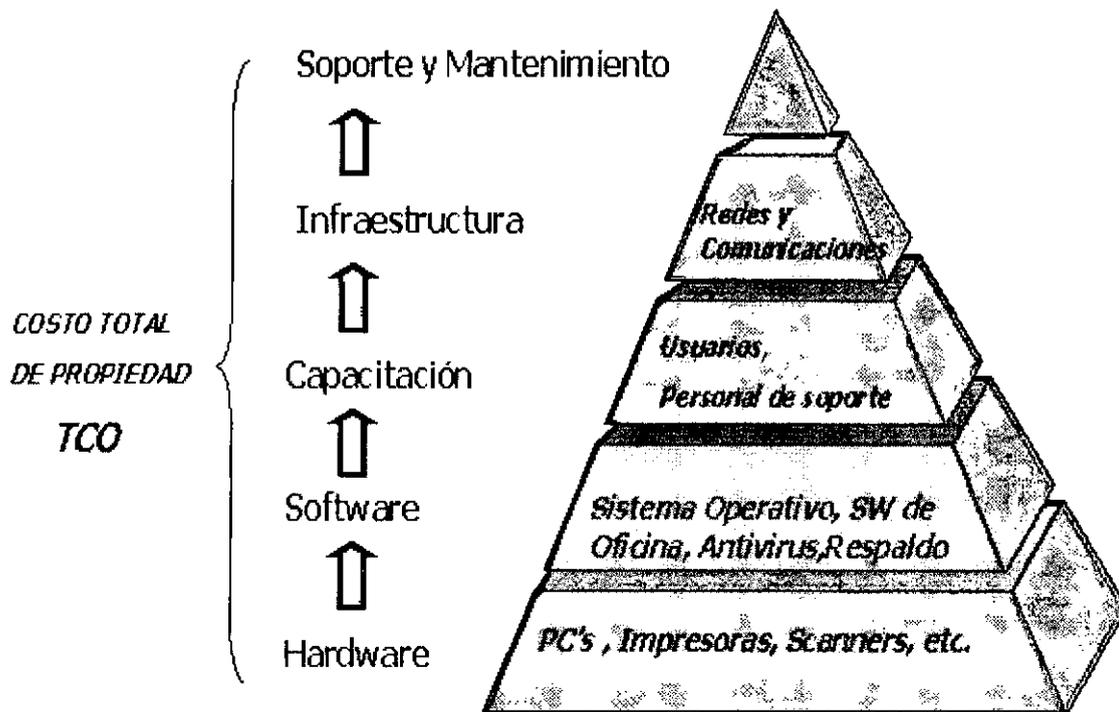
---

**Costo de adquisición del paquete de Software:** es el costo del programa en si, y es el componente principal, a tener en cuenta, ya que es el usualmente definitivo a la hora de decidir la posterior compra o no de la herramienta en cuestión.

**Costo de las licencias necesarias para utilizar el paquete:** Es un dato muy útil, no solo para el cálculo del costo de las licencias del programa, propiamente dicho, sino también para asociar los costos de las licencias del software de base (si es que el programa no corre en el sistema operativo que tenemos licenciado).

**Costo de futuras actualizaciones o modificaciones:** Toda herramienta de software debe adaptarse al continuo y a veces vertiginoso cambio en el mundo de la informática. El costo de actualizar el software, para adaptarlo al cambio de tecnología o de realizar modificaciones en el mismo, debe quedar claramente definido antes de decidir la compra y es otro de los factores importantes que deciden la compra de una u otra.

**Costo de soporte:** Es necesario dejar bien en claro antes de adquirir un determinado paquete, la garantía, el servicio de soporte y los costos del mismo, a cargo de quién corren.

**Costos de Software:**

El Software es un componente muy importante del costo de todo el Parque Informático, como vemos se encuentra casi en la base de esta pirámide apenas por encima del de Hardware.

Existen asociados al costo del Software costos directos e indirectos a saber:

**Costos Directos:**

- *Adquisición:* Costo de la compra del paquete de Software propiamente dicho.
- *Depreciación:* En el caso de Software, la depreciación se produce debido a la desactualización que sufren los paquetes, distinta a la sufrida por un bien de uso, es decir una herramienta de software no se desgasta, pero pierde valor debido a la aparición de nuevas necesidades en la APP o bien por el surgimiento de necesidades no contempladas originalmente, por los diseñadores.

## ADMINISTRACIÓN DE SOFTWARE

---

- *Alquiler:* Algunas herramientas de software no se venden sino que son cedidas a la APP mediante el pago de una suma por un período determinado. Ej. Mensual, semestral, Anual, etc.
- *Capacitación:* La compra de un nuevo programa genera la necesidad de invertir en la preparación del personal que tendrá a cargo el manejo del mismo.

### **Costos Indirectos:**

- *Costos de Operación:* todos los que se producen por la propia puesta en marcha del sistema.
- *Costos producidos por eventual falta de disponibilidad:* Hacen referencia a todo lo que se pierde si el sistema deja de funcionar, ya sea pérdida de ganancia normalmente conocido como costo de oportunidad o ya sea pérdidas concretas, como multas por no brindar servicio, etc.

Todos estos costos deben ser tenidos en cuenta a la hora de contrastar con los beneficios de cada herramienta y eventualmente decidir la compra o no de la misma.

### **Beneficios:**

Indudablemente no todos son costos en materia de software para la APP, sino que es necesario analizar los beneficios, para así lograr tener fundamentos a la hora de decidir una compra de manera adecuada.

Estos son inherentes al tipo de herramienta a adquirir, por lo que no se puede detallarlos de manera específica, pero siempre tendrán algunas de las siguientes características:

- Automatización de tareas administrativas.

- o Control de stock
- o Acceso rápido a datos
- o Etc.

Como puede observarse a simple vista es muy difícil cuantificar este tipo de beneficios, será una tarea a realizar en conjunto entre el interesado en el sistema y la Gerencia de Tecnología, debiéndose para esto analizar en cuanto beneficiará cada uno de los puntos a cada repartición en particular para obtener una medida monetaria del beneficio, la cual será contrastada oportunamente.

De la comparación entre costos y beneficios surgirá la decisión de la compra o no.

#### **Reasignación de Programas:**

Luego de un estudio realizado en diferentes dependencias de la APP se verificó que existe una gran resistencia a la reasignación de Paquetes dentro de la APP, sin embargo, proponemos este sistema de trabajo para las dependencias que tengan Software debidamente licenciado sin utilizar.

Las reparticiones que posean algún software no utilizado, deberán comunicarlo a la Gerencia de Tecnologías de la Información (GTI), quién llevará un registro actualizado del mismo; al plantearse la necesidad de adquirir nuevo software cada dependencia se dirigirá a la GTI, quien será el organismo a cargo de autorizar la adquisición de todo el software. En el caso de necesitarse un paquete de los no utilizados se propondrá a la dependencia solicitante la alternativa de utilizar el mismo.

#### 4. ESTANDARIZACIÓN

Para poder cumplir con la misión de tener un control adecuado de los costos en cuanto a la adquisición de software es necesario cumplir con una serie de puntos:

Una forma de reducir al mínimo los costos de adquisición de software es identificar y comunicar las necesidades de software actuales y futuras de la APP, la presupuestación para la adquisición de software y la compra solamente de lo que es necesario en conformidad con procedimientos de compra claramente identificados.

La preparación del presupuesto es vital. Deben identificarse los gastos planificados de software como una partida separada dentro del presupuesto para Tecnología Informática (TI) y realizar el seguimiento de los gastos actuales en comparación con los proyectados. De esta manera se puede evaluar en forma adecuada sus necesidades, garantizar que el software adquirido sea legítimo y planificar futuras adquisiciones.

Un proceso de administración del software permite a una organización identificar y comunicar a sus empleados el software que actualmente utiliza, así como las actualizaciones esperadas, las sustituciones, las eliminaciones y las políticas para retención de datos y programas. Al recopilar y distribuir esta información, es posible administrar software, datos y archivos de programas de manera sistemática y ocasionar inconvenientes mínimos. Por otra parte, la eliminación sin sobresaltos del software que ya no se utiliza libera espacio del equipo informático existente y, de esta manera, ayuda a las organizaciones a evitar los costos de actualizar o reemplazar innecesariamente el equipo informático.

### **Controlar los costos de mantenimiento de software**

Al identificar las necesidades presentes y futuras de la APP, y especificar cuándo el software dejará de ser utilizado, es posible controlar el costo de mantenimiento para el software y evitar el costo implícito en la renovación de licencias innecesariamente o en términos demasiado amplios. Es posible realizar el control mediante un proceso de administración que estudie de manera periódica las necesidades de software de la organización, actualizando periódicamente la lista de software utilizado y comunicando claramente por adelantado cuándo diferentes aplicaciones y versiones dejarán de ser utilizadas y, en tal caso, retirarlas de las computadoras de la APP.

### **Evitar procesos legales, sanciones y multas**

Es posible para la APP los costos de los procesos legales, las multas y las sanciones mediante la puesta en vigor del proceso de administración de software descrito en este documento. El proceso generará un registro de los documentos necesarios para evitar estos costos.

### **El registro incluirá:**

- Una declaración escrita de la política de software de la APP
- Pruebas de la aceptación y el entendimiento por parte de los empleados de la política, el proceso de administración y las responsabilidades
- Un inventario completo y actual de los activos de software
- Documentación sobre todas las medidas adoptadas en apoyo del proceso de administración.

## MEJORAR EL RENDIMIENTO

Además de un control más eficaz de los activos, el cual mejora el rendimiento de todas las organizaciones el plan de administración de software incluirá:

- Garantía de la calidad y fiabilidad del software
- Maximización de la compatibilidad de los recursos de TI
- Anticipación y aprovechamiento del cambio
- Aumento de la productividad de los empleados

## Garantizar la calidad y confiabilidad del software

Un proceso eficaz para la administración del software garantizará la calidad y fiabilidad del software.

Permite identificar adecuadamente, evitar y eliminar (cuando se encuentran instaladas en las computadoras de la organización) las copias ilegales de software – las cuales pueden ser defectuosas o estar infectadas con virus, ser obsoletas, o pertenecer a una versión reciente pero no probada adecuadamente - . Por otra parte, el software con licencia ofrece garantía de autenticidad y calidad del producto, garantía del autor del software, documentación, manual de instrucciones, tutoriales, soporte del producto (incluida la información sobre actualizaciones los servicios para la solución de problemas) y formación.

## Algunas reglas que deben ser tenidas en cuenta

- Ningún empleado instalará o distribuirá software para el cual la APP carezca de la licencia apropiada.
- Ningún empleado instalará actualizaciones de software en una computadora que no tenga instalada ya una versión original del software. El Jefe de

## ADMINISTRACIÓN DE SOFTWARE

---

Información o el empleado designado destruirá la copia del software actualizado

El Jefe de Información o el empleado designado destruirán todas las copias de software obsoleto o para el cual la organización carezca de la licencia correspondiente. Como alternativa, el Jefe de Información puede obtener las licencias necesarias para conservar el software no autorizado en las computadoras de la organización.

Se debe establecer y mantener un sistema de registro para las licencias de software, el equipo informático, los CD Rom originales y los disquetes, la información para el usuario, y la información de comprobación en un lugar seguro, centralizado. Asimismo debe considerar el uso de programas de computadora para administración de software a fin de realizar de manera automática los mencionados registros.

### 5. CONCLUSIÓN

El Software para computadoras tiene asociados Beneficios y Costos, tanto directos como indirectos, derivados de los primeros, los cuales deben ser tenidos en cuenta. Es una alternativa a considerar la reasignación de Software por cuanto el ahorro que supone es grande y no puede ser omitido.

## **PROGRAMA DE MANTENIMIENTO**

### **1. PROGRAMA DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO**

El mantenimiento como ya se mencionó puede en la práctica ser de dos tipos diferentes, *preventivo* (actuar antes de que se produzca el problema, por lo tanto evitar el trastorno que implica una rotura de hardware), o *correctivo* (actuar después de que se produce el fallo, es decir reparar una avería ya producida). En este programa se pretende definir la combinación óptima de opciones que hace mínimo el costo del mantenimiento combinando la tercerización del mantenimiento en el caso de equipos propietarios, con el mantenimiento a cargo de un grupo perteneciente a la propia APP, para el resto de los equipos que no estén cubiertos en algún tipo de garantía.

A continuación se definirán las condiciones mínimas necesarias para el procedimiento de mantenimiento, las cuales deberán aclararse en el contrato o pliego correspondiente, en el caso de tratarse de una licitación de mantenimiento.

Se deberá contar con autorizaciones administrativas previas para realizar paradas preventivas o de diagnóstico.

A pesar de que el contrato de mantenimiento especifique paradas preventivas o de cualquier otra índole, el licitante deberá programar de acuerdo con el cliente estas actividades, con el fin de entorpecer lo menos posible las labores de la organización.

Se podrán determinar horarios especiales y periodicidades mínimas para este tipo de paradas.

**PROGRAMA DE MANTENIMIENTO**

---

**Sustitución de piezas**

- o Solamente se admitirán repuestos nuevos o reciclados convenientemente, y se procurará que sean los recomendados por el fabricante del equipo.
- o Si no existen piezas disponibles, se deben plantear soluciones alternativas, como el cambio o sustitución de los equipos por cuenta del licitante.
- o La sustitución de equipo físico de almacenamiento implica la restitución de la información almacenada, es aconsejable dejar esto plasmado en el correspondiente Pliego.
- o Los gastos de transporte de piezas o máquinas deberán estar incluidos en el contrato.
- o La empresa licitante podrá ofertar la sustitución de equipos obsoletos, que sea más caro mantener, por otros más modernos o en mejores condiciones de uso siempre que garanticen prestaciones iguales o superiores a las del equipo sustituido.
- o La organización podrá especificar de quién será la propiedad de las piezas sustituidas, habitualmente recaerá en el mantenedor, pero puede pactarse lo contrario.
- o Se podrá valorar que el licitador asuma la reposición de fungibles y consumibles, pero para ello es recomendable informarle en el Pliego de los niveles de uso y producción de los equipos.

**Estado inicial de las máquinas**

La Administración podrá obligar a las empresas licitantes a aceptar el estado actual de las máquinas como válido, recomendándose que la mayoría de ellas cumplan las especificaciones del fabricante en cuanto a estado de mantenimiento.

Puede resultar muy interesante el describir el estado del equipo o su antigüedad.

### **Requisitos organizativos a las empresas licitantes**

Especificaciones para la presencia de personal del mantenimiento en las instalaciones de la APP. Se podrá definir en el pliego correspondiente la necesidad de contar con un número determinado de personas y su grado de capacitación técnica, pertenecientes a la empresa licitante en las propias instalaciones de la APP, para atender los requerimientos de manera eficiente.

En cuanto al procedimiento para comunicar a la empresa adjudicataria la necesidad de un servicio. Se debe definir explícitamente en el pliego de licitaciones, y quedar muy en claro un mecanismo para que ambas partes tengan una constancia de la fecha y hora de cada reclamo, y establecer la existencia o no de moras en el servicio, el medio a elegir deberá cumplir con los siguientes requisitos:

- Registrar el día del reclamo y la hora del mismo.
- Registrar la persona que efectúa el pedido.
- Establecer un mecanismo de prioridades para categorizar reclamo o pedido.

Un medio que cumple estos requisitos y además tiene como valor agregado el bajo costo es el correo electrónico, pero se pueden aceptar otros, siempre teniendo en cuenta el cumplimiento de los requisitos arriba mencionados.

### **Requisitos sobre almacenamiento y distribución de repuestos.**

Se deberá documentar cada actividad, exigiendo para ello: partes e informes obligatorios. Ejecución de estadísticas de actividad y fallos por marca y modelo, etc. Existe asimismo la posibilidad de crear una base de datos de incidencias, para lo que habrá que exigir las estadísticas o informes en un formato apropiado.

### **Requisitos sobre confidencialidad de datos almacenados en equipos**

Deberá garantizarse que no se utilice la información contenida en algún medio magnético, se establecerá claramente en los pliegos de condiciones la forma de protegerse de estos robos de información, que pueden ser de gran impacto dentro de la APP.

### **Reparación de equipos**

Las reparaciones de equipos físicos contribuyen en un elevado porcentaje al coste de un contrato de mantenimiento. Por esta razón, se debe realizar la especificación en el contrato de cláusulas que ayuden a disminuir estos costes importantes para la economía de la APP.

El coste de la reparación de un equipo se compone de los costes de los siguientes elementos:

- Diagnóstico.

La identificación del problema es una actividad que en la mayor parte de los casos consume bastante tiempo y, por tanto, dinero. Para disminuir este tiempo, no es suficiente con especificar cláusulas limitadoras de tiempos, además de esto. Es conveniente exigir que las empresas encargadas de brindar el servicio de mantenimiento sigan los procedimientos que definen los fabricantes del equipo, y que posean todas las herramientas de diagnóstico, manuales, etc, recomendadas por ellos.

- Sustitución (posible) de piezas.
- Mano de obra de reparación.
- Desplazamientos.

**PROGRAMA DE MANTENIMIENTO**

---

Existen dos tipos de gastos de desplazamiento:

- o Desplazamiento de operarios.
- o Desplazamiento de equipos.

Cuando no sea posible cumplir los tiempos de reparación especificados y, por lo tanto, exista un indisponibilidad del equipo demasiado grande, el licitante deberá proponer una solución que permita a la organización continuar con sus labores habituales como, por ejemplo, la sustitución temporal del equipo averiado, y el traspaso de la información que hiciere falta desde el equipo averiado al provisto por el licitante.

## 2. ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE MANTENIMIENTO

En este punto se pretende dar la orientación suficiente a la APP para la preparación del conjunto de especificaciones que definirán los requisitos que han de cumplir las empresas que ofrezcan los servicios de mantenimiento de equipos físicos objeto de la contratación.

Se realiza en primer lugar un análisis de las necesidades del comprador, a continuación se recogen los factores relevantes a tener en cuenta en el proceso de contratación y, finalmente, se describe cómo deben ser planteadas las especificaciones técnico-funcionales para la elaboración del Pliego de Prescripciones Técnicas, qué normas, estándares y cláusulas tipo pueden ser de aplicación, y cuál es el cuestionario técnico diseñado para normalizar las ofertas y facilitar su evaluación.

### **Análisis de las necesidades de la APP**

Las necesidades de la APP de mantenimiento de equipos físicos son muy variables, como consecuencia de la diversidad de máquinas existentes en la organización.

Para el responsable público, el fin de la actividad de mantenimiento es:

- Limitar al máximo posible cualquier tipo de período de inactividad.
- Mantener los equipos en buen estado funcional para que las nuevas adquisiciones se encuentren con un entorno receptivo que no obligue a costosas reconfiguraciones y/o adaptaciones.

Se precisa, pues, una planificación de las necesidades reales de mantenimiento para lograr un equilibrio entre el servicio a prestar por los equipos y su coste de mantenimiento. Las actividades de mantenimiento preventivo y/o correctivo de equipos físicos más normales son las limpiezas, revisiones y diagnósticos, reparaciones y cambios de piezas. En cuanto a las limpiezas, hay que subrayar el alto coste que suponen, por lo que se debe estudiar bien su periodicidad, necesidad e intensidad. Estas características deben exigirse en función de los servicios reales que prestan los equipos y su nivel de criticidad.

Se puede dividir este apartado en los siguientes subgrupos:

- **Sistemas no propietarios**

Se considerarán aquí aquellos sistemas, sin importar su tamaño, que no contienen una tecnología dominada por un solo fabricante, de forma que su mantenimiento pueda ser objeto de competencia pública más o menos extensa. Dentro de estos sistemas pueden encontrarse desde procesadores paralelos hasta servidores de pequeñas RALs (Redes de Área Local), pasando por sistemas periféricos de impresión, etc.

## PROGRAMA DE MANTENIMIENTO

---

Por otro lado, también se considerará todo lo relacionado con la microinformática: Impresoras y periféricos de todo tipo, PCs y compatibles, consumibles, etc.

### **Sistemas propietarios**

Existen múltiples componentes en cada sistema propietario que pueden estropearse: procesador, sistemas de almacenamiento masivo, sistemas de refrigeración, etc. Puede (debe) incluirse el mantenimiento del sistema operativo y otro equipo lógico muy básico junto con el equipo físico, como si fuese una pieza más.

Los costes de este tipo de mantenimiento son una de las razones que promueven lo que se llama ajuste dimensional (rightsizing). Este concepto es la evolución de downsizing, el cual apareció en los años 80 cuando se descubrieron las posibilidades de ahorro que ofrecía la arquitectura cliente-servidor, al utilizar redes de comunicaciones combinadas con microordenadores para sustituir a los grandes sistemas. Esta fiebre desembocó en algunos fracasos, lo que produjo el cambio de orientación de búsqueda de reducción de tamaño y precio a búsqueda del tamaño y precio adecuados.

Necesidades comunes extras que se incluyen en contratos de mantenimiento de este tipo de equipos son:

- o Revisiones del microcódigo de los chips, tarjetas, firmware, etc., incluidos con los equipos. El microcódigo es el conjunto de programas que actúa directamente sobre circuitos eléctricos o electrónicos, usualmente contenidos en pequeñas memorias de sólo lectura y que se ejecutan como rutinas de diagnóstico o de iniciación (aunque pueden tener otros usos) al encender los equipos físicos. Este tipo de equipo lógico es vital para el correcto funcionamiento de equipos físicos. Su actualización se considera parte del

**PROGRAMA DE MANTENIMIENTO**

---

mantenimiento de equipos físicos, porque su función está completamente relacionada con el funcionamiento del equipo físico.

- o Instalación de las actualizaciones y versiones que aparezcan durante el período de prestación de servicio como deber del contratista, indicando el coste en su caso. Con esta cláusula se restringe en la práctica la competencia ya que el propietario del software es el que mejor puede llevar a cabo las actualizaciones y versiones del mismo.
- o Realización de inventarios, estadísticas, etc, por equipos, marcas y modelos, que sirvan para predecir y planificar futuros contratos y/o adquisiciones.

Aunque se pretenda sacar a concurso sistemas propietarios, no debe incluirse en el mismo lote varios sistemas propietarios diferentes. Esto facilita la competencia y no perjudica al comprador público, dado que una empresa puede presentarse a varios lotes a la vez.

**Factores relevantes en el proceso de contratación**

En la definición del objeto del contrato y los requisitos inherentes al mismo así como en la valoración y comparación de ofertas de los licitadores pueden intervenir muchos factores y de muy diversa índole.

Es de suma importancia que todos los factores relevantes que intervienen en el proceso de contratación queden debidamente recogidos en el pliego de prescripciones técnicas que regule el contrato.

Se mencionan a continuación algunos factores que pueden intervenir más decisivamente en el proceso de contratación de mantenimiento de equipos físicos, y cuyo seguimiento debe efectuarse exhaustivamente.

- Incremento del número de equipos a mantener sin coste adicional.

**PROGRAMA DE MANTENIMIENTO**

---

Durante el período de prestación del servicio existe la posibilidad de que equipos que permanecen en garantía al comienzo del mismo dejen este estado. Se valorará especialmente la inclusión de estos equipos automáticamente en la relación inicial, sin coste alguno para el cliente. Este incremento deberá ser cuantificado para lo cual se incorporará la información necesaria en los anexos del Pliego correspondiente.

- Inclusión de fungibles y/o consumibles.

Se valorará que el licitante contemple hacerse cargo de todos los componentes de cualquier equipo, incluyendo el material fungible y consumible. Los fungibles son todos los componentes asociados con la operación de los equipos que deben ser periódicamente sustituidos. Se diferencian de los consumibles porque éstos desaparecen con el uso, mientras que los primeros implican algún tipo de residuo. De este material pueden hacerse excepciones (papel, discos flexibles...) de acuerdo entre la Administración y el licitante. La empresa adjudicataria generará las reservas necesarias de material fungible en cada centro para garantizar el funcionamiento normal de los correspondientes equipos. La Administración podrá incluir medidas estadísticas del consumo de estos materiales en el pliego de prescripciones técnicas.

- Mantenimiento de equipos antiguos.

Para muchos equipos en servicio puede ser complicado o antieconómico encontrar piezas de recambio adecuadas. El licitante podrá optar, de acuerdo con la organización, por el cambio de estos equipos por otros más modernos de igual o superior funcionalidad, u otros de mejor estado de uso con prestaciones iguales o superiores a los sustituidos.

- Rapidez de reparación.

### PROGRAMA DE MANTENIMIENTO

---

Cualquier disminución que ofrezca la empresa licitante en los tiempos de respuesta, reparación, etc, sobre el valores correspondientes que se establecen en las cláusulas del pliego de prescripciones técnicas debe ser valorado positivamente.

- Respuesta a urgencias fuera de horario.

En muchas ocasiones, la organización no dispondrá de recursos para contratar un mantenimiento de 24 horas, lo que no quiere decir que no puedan existir incidencias fuera del horario contratado. La disposición por parte del licitante a responder a casos de emergencia, fuera del horario habitual, con el mínimo coste para la organización, debe ser valorada positivamente.

- Implantación geográfica.

La estructura descentralizada de muchas organizaciones impone sobre el licitante la obligación de atender incidencias dispersas geográficamente por todo el territorio nacional. Es posible que distintos licitantes ofrezcan tiempos de respuesta superiores al máximo para centros alejados. El responsable público debe verificar cuál es la estructura geográfica de la empresa licitante para asegurar que los tiempos de respuesta que ofrezcan puede ser cumplidos en la práctica. Hay que tener en cuenta que la penalización económica (por retraso en el servicio) que pueda sufrir la empresa licitante puede no compensar el daño causado por la no prestación de un servicio de reparación en un momento crítico.

- Mantenimiento y monitorización a distancia.

Este factor está relacionado con el anterior. Las modernas tecnologías de comunicación pueden resolver el problema geográfico con medios de comunicación eficientes que permitan el envío de alarmas, la monitorización de los equipos y el conocimiento de las averías. Sin embargo, el licitante debe tener la suficiente

**PROGRAMA DE MANTENIMIENTO**

---

infraestructura, metodología y organización para poder dar un servicio eficaz a distancia que resuelva los problemas detectados.

- Metodología.

La aplicación de una metodología específica de trabajo es un factor relevante y diferenciador entre empresas.

### 3. CONCLUSIÓN

El proceso de mantenimiento de equipos físicos puede ser dividido en dos aspectos: Mantenimiento Preventivo (antes de producida la falla, evitar que la misma se produzca) y Mantenimiento Correctivo.(después de producida la falla, intentar repararla), ambos aspectos deben ser balanceados, porque si bien es preferible realizar solamente mantenimiento preventivo, el costo de esta postura sería prohibitivo, por lo tanto se debe buscar un punto medio en que las fallas se produzcan en los equipos no vitales, y que se realice mantenimiento preventivo para evitar los fallos de equipos que harían venir abajo el trabajo de toda la APP.

Se arriba a la conclusión de que la APP debe poseer un grupo interno de mantenimiento para atender los requerimientos de computadoras personales no cubiertas por garantías o servicios contratados por cada ministerio, y contratar un servicio de mantenimiento privado para los servidores, centrales telefónicas, y otro equipamiento de tipo propietario, en el cual cada empresa mantiene su propio equipo y lo hace mejor que su competencia.

**SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO**

---

**SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO**

1. **PROGRAMA DESARROLLADO A MEDIDA**

Se realizó un análisis diseño y programación de un programa desarrollado a Medida, denominado Inventario 1.0. El cual fue desarrollado en Power Builder, y Utilizando bases de Datos compatibles con cualquier motor de Base de Datos, tales como Microsoft Access 2000.

Debido a los altos costos que implica el licenciamiento de un programa de las características de Arca Inventory & Auditing V.2.3, se desarrollo un programa a medida, contando con la colaboración del Grupo de programación de la Secretaría de Tecnologías de la Información, y es la opción que más se ajusta en nuestro caso, ya que es posible obtener un buen producto a un costo realmente bajo para la provincia.

2. **MANUAL DE INSTALACIÓN**

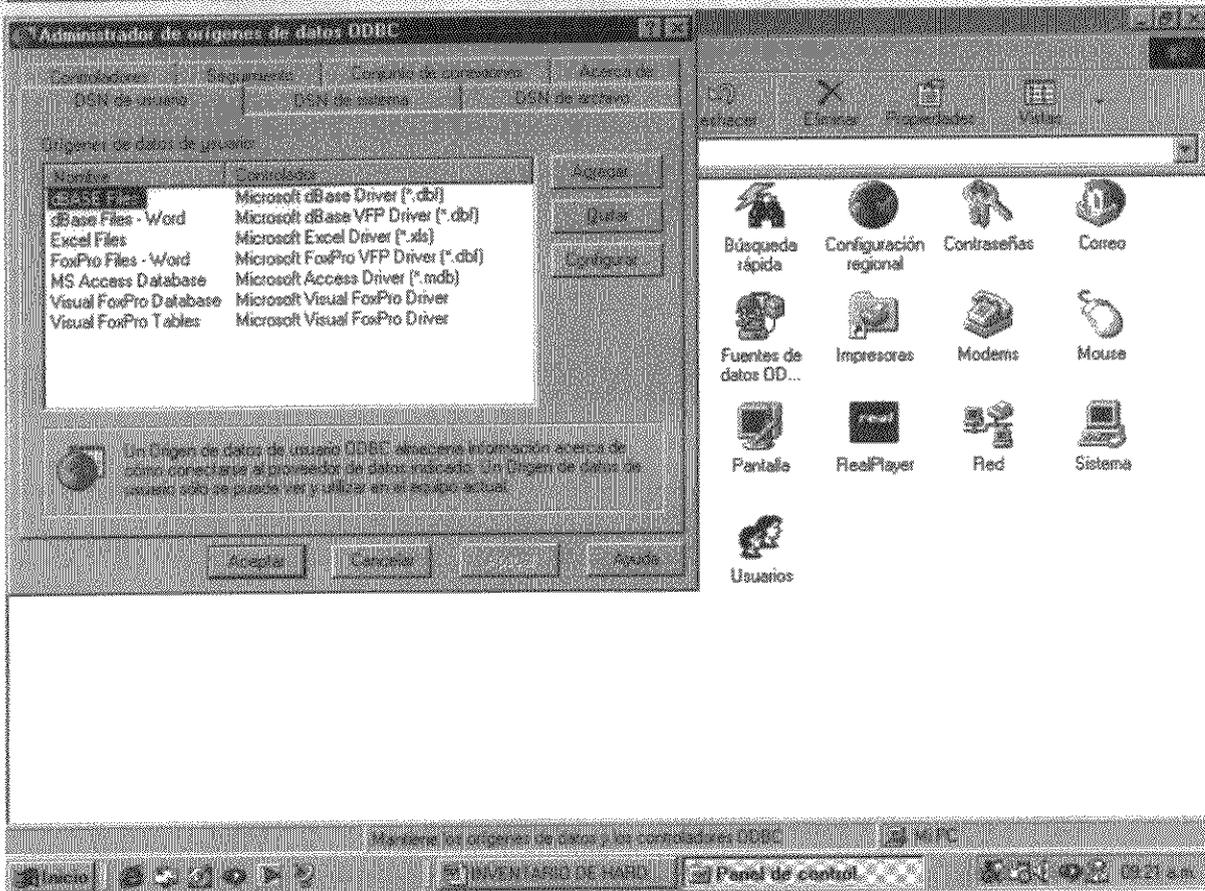
**Recolección Manual**

Insertar el CD y ejecutar el programa SETUP.EXE que se encuentra en el subdirectorio Instalador.

Crear el OBDC (Orígenes de Datos) llamado Inventario

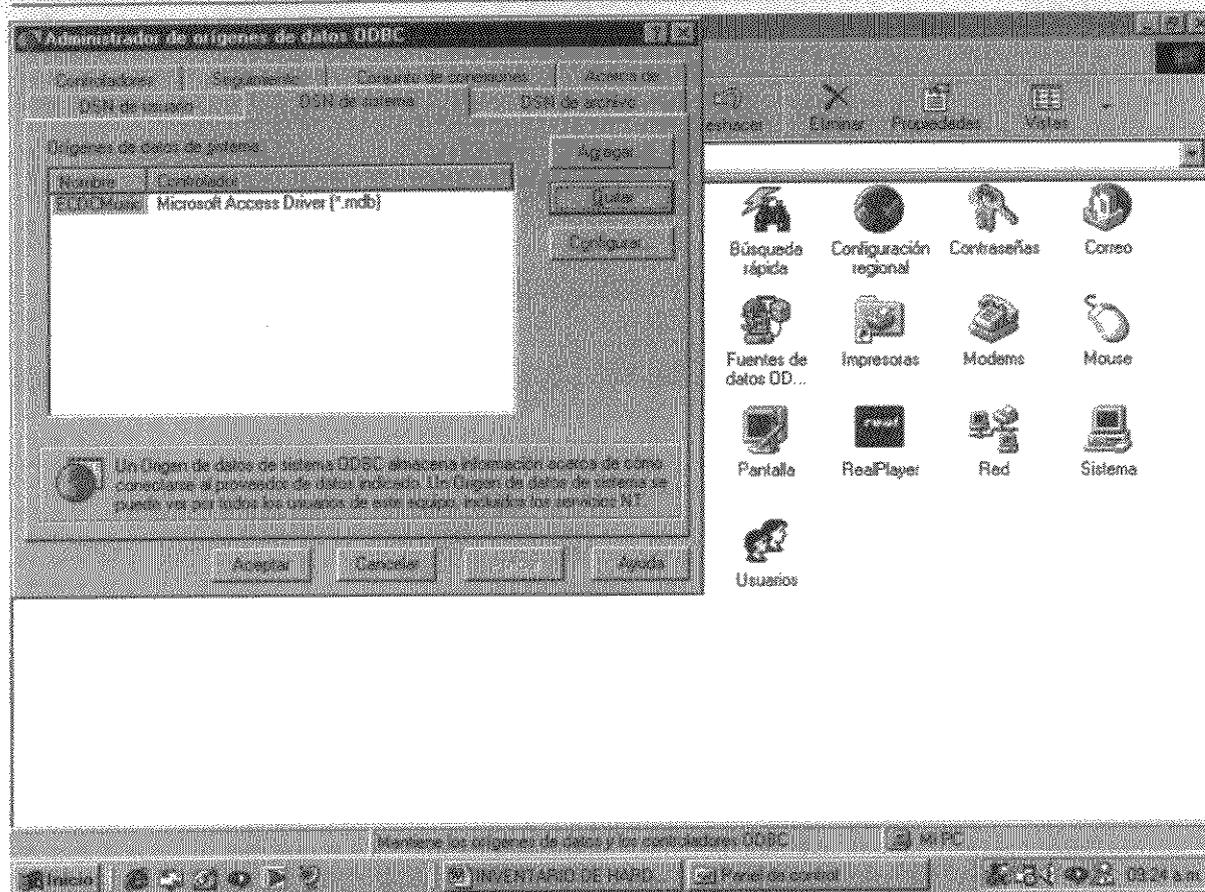
Haga clic en Inicio, seleccione Configuración y , a continuación haga clic en Panel de Control en Windows 2000 haga doble clic en Herramientas Administrativas y a continuación en Orígenes de Datos (ODBC), en Windows 98, 95 haga clic en Fuente de Datos (ODBC)

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



Haga clic en la pestaña DSN de Sistema

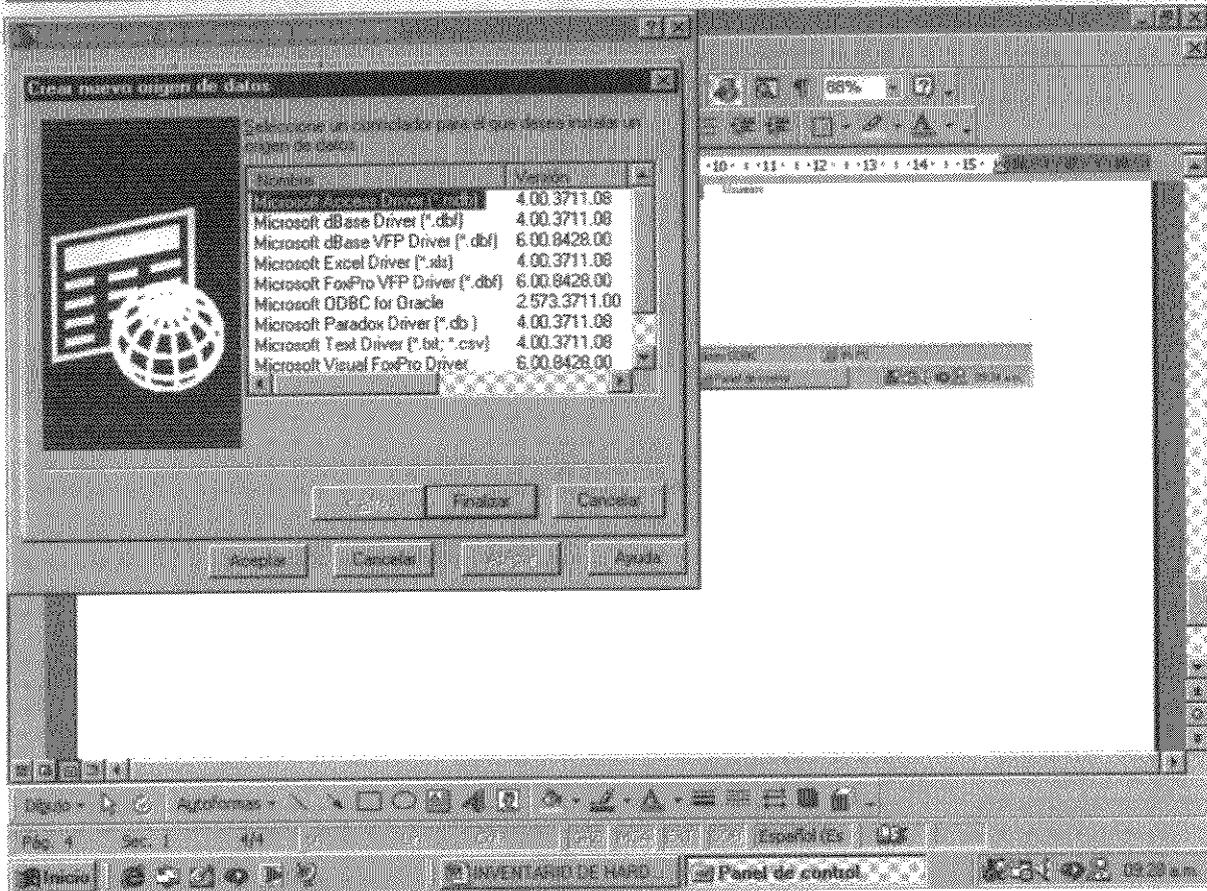
SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



Haga clic en el botón Agregar

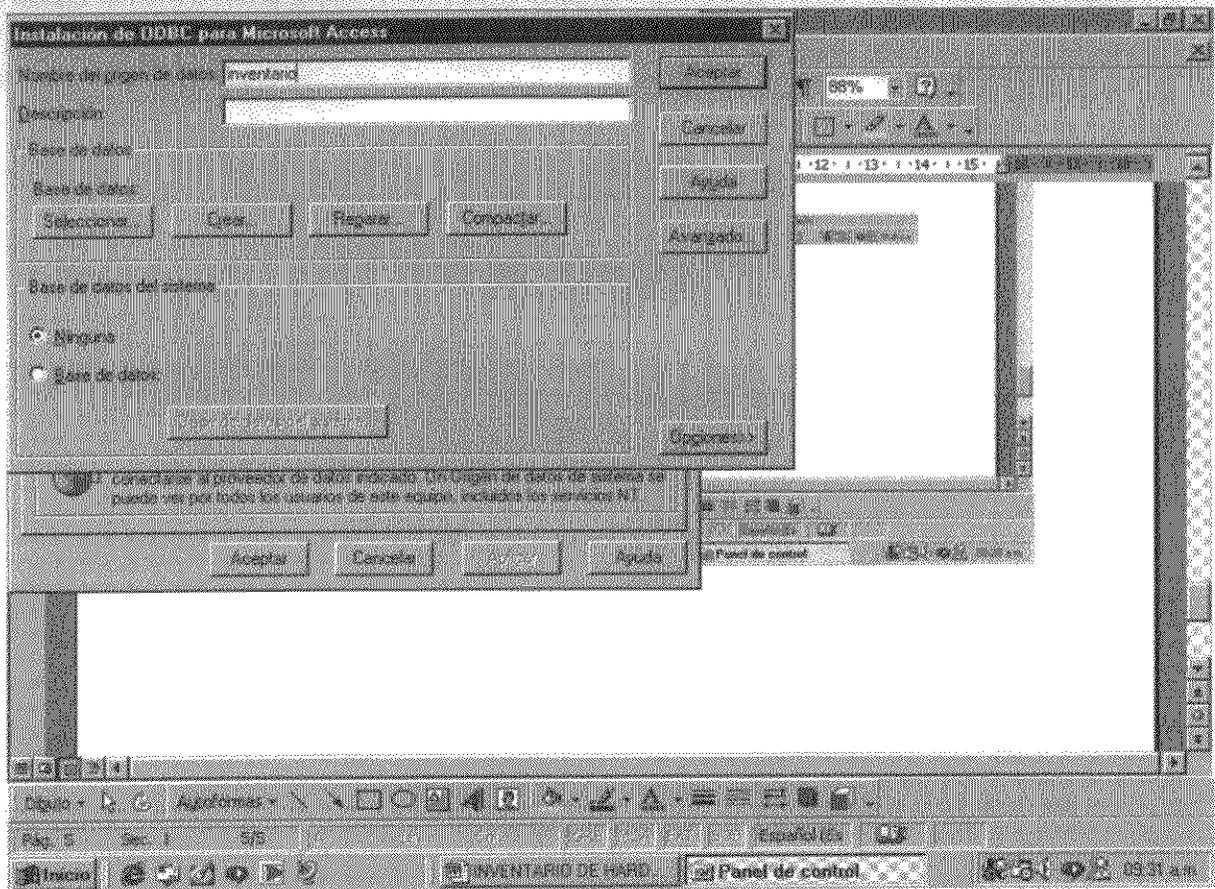
Seleccione Microsoft Access Driver (\*.mdb)

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



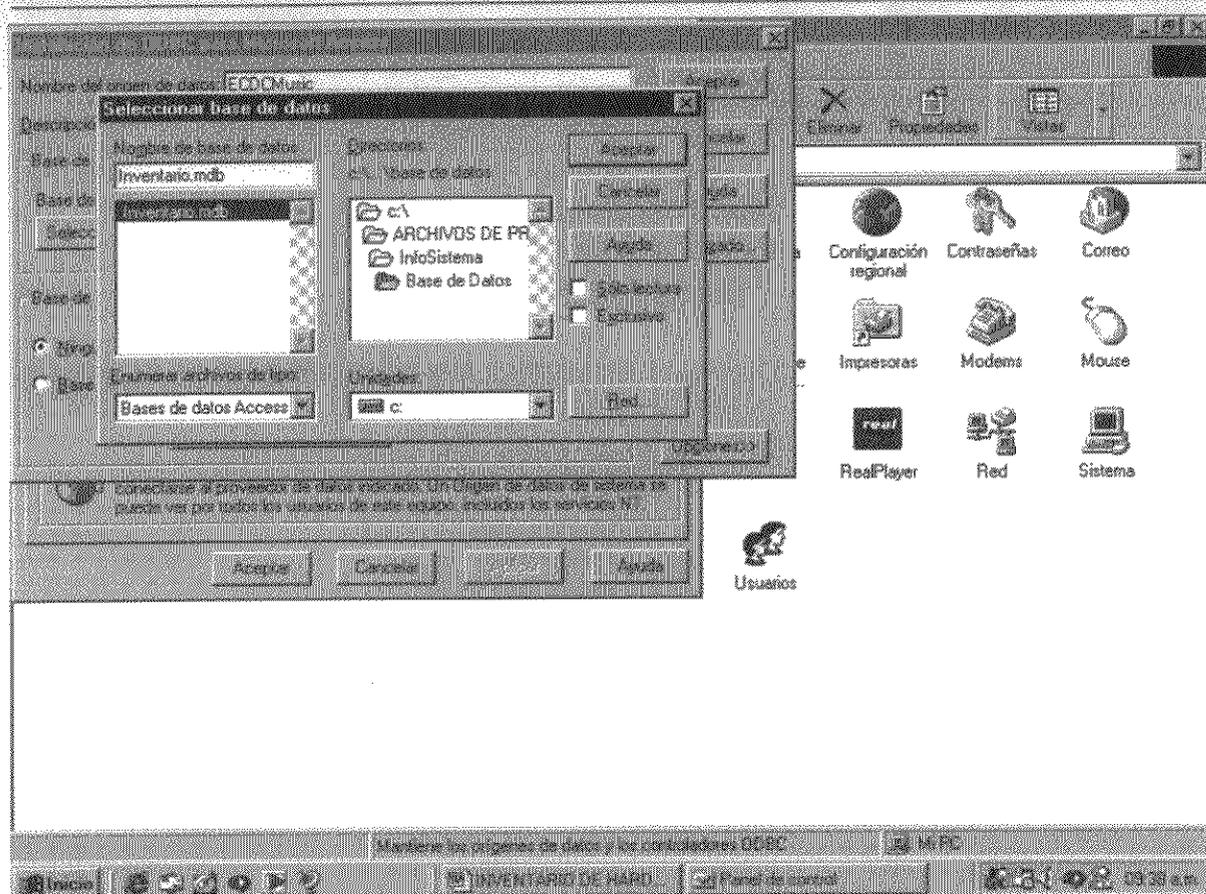
Colocar como nombre del origen de datos: inventario

SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



Haga clic en el botón Seleccionar del Marco Base de Datos, abrir la Carpeta Archivo de Programa y Seleccione la Carpeta InfoSistema y dentro de él la Carpeta Base de Datos. Por ultimo seleccione el archivo *INVENTARIO.MDB*

## SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



3. Por ultimo acceder a Inicio y dentro de él acceder a Programas y dentro de éste buscar INFOSISTEMA y haga doble clic de INFOSISTEMA.

Una vez dentro del Sistema hacer clic en Carga de Datos y Agregar la Información del Equipo con el cual se esta trabajando.

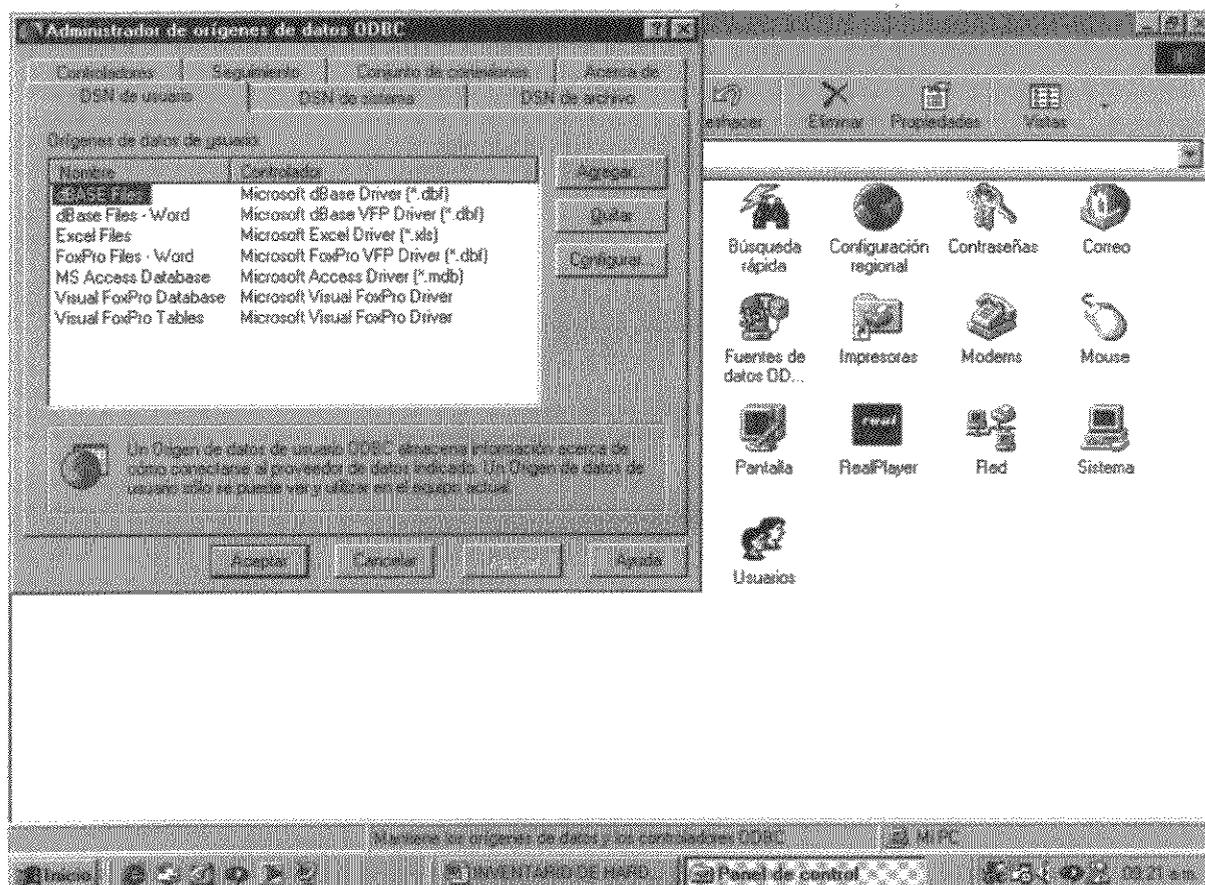
### Forma Remota

Seleccione Entorno de Red, localizar la máquina donde se encuentra el instalador y ejecutar el archivo SETUP.EXE.

2. Crear el ODBC (Orígenes de Datos) llamado Inventario

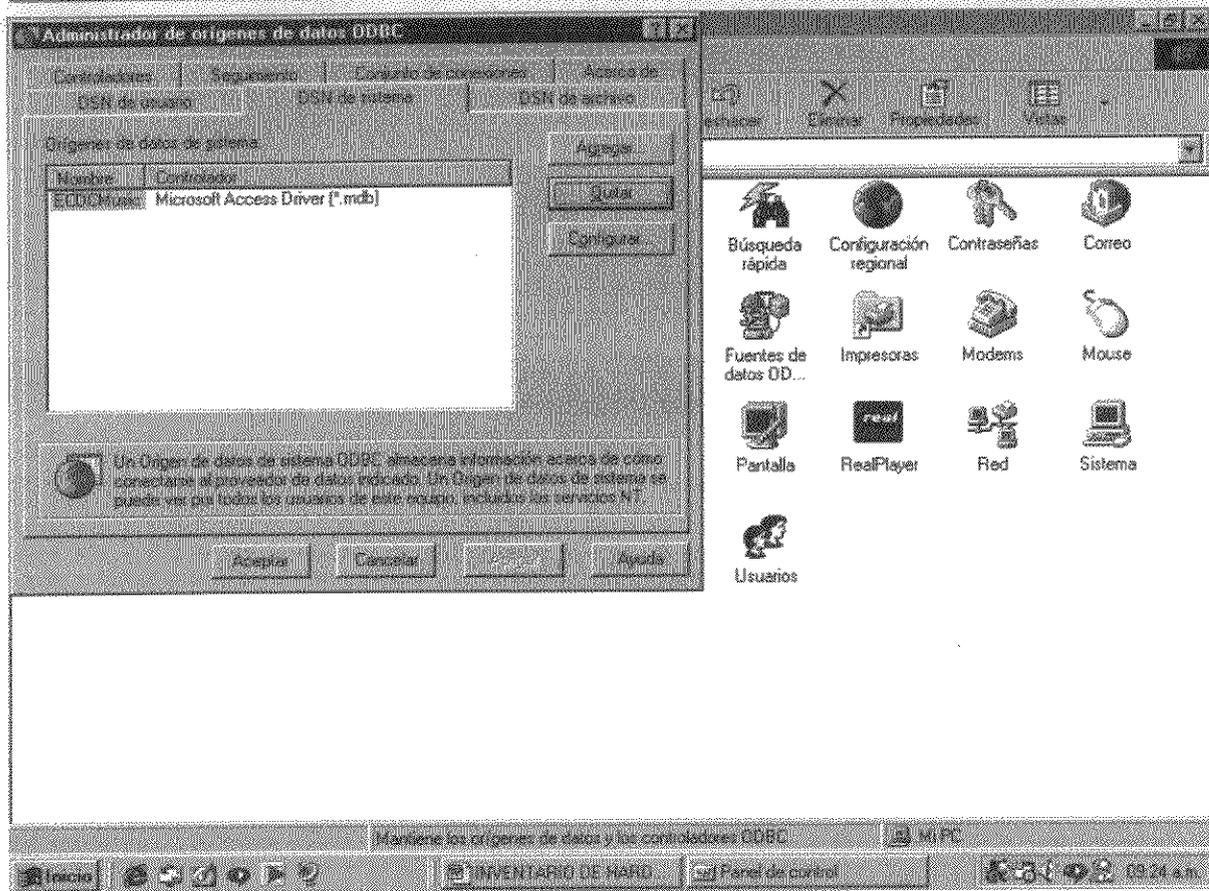
## SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO

Haga clic en Inicio, seleccione Configuración y , a continuación haga clic en Panel de Control en Windows 2000 haga doble clic en Herramientas Administrativas y a continuación en Orígenes de Datos (ODBC), en Windows 98, 95 haga clic en Fuente de Datos (ODBC)



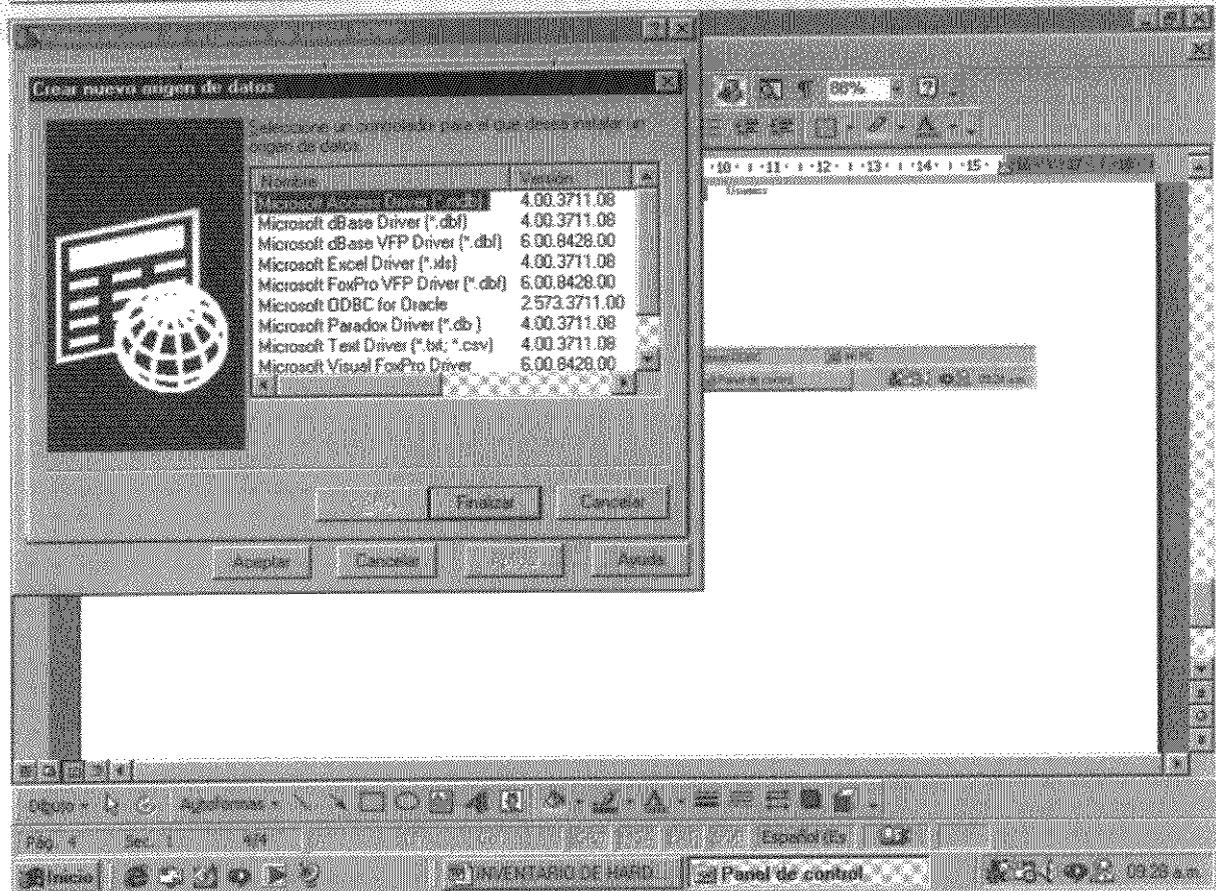
Haga clic en la pestaña DSN de Sistema

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



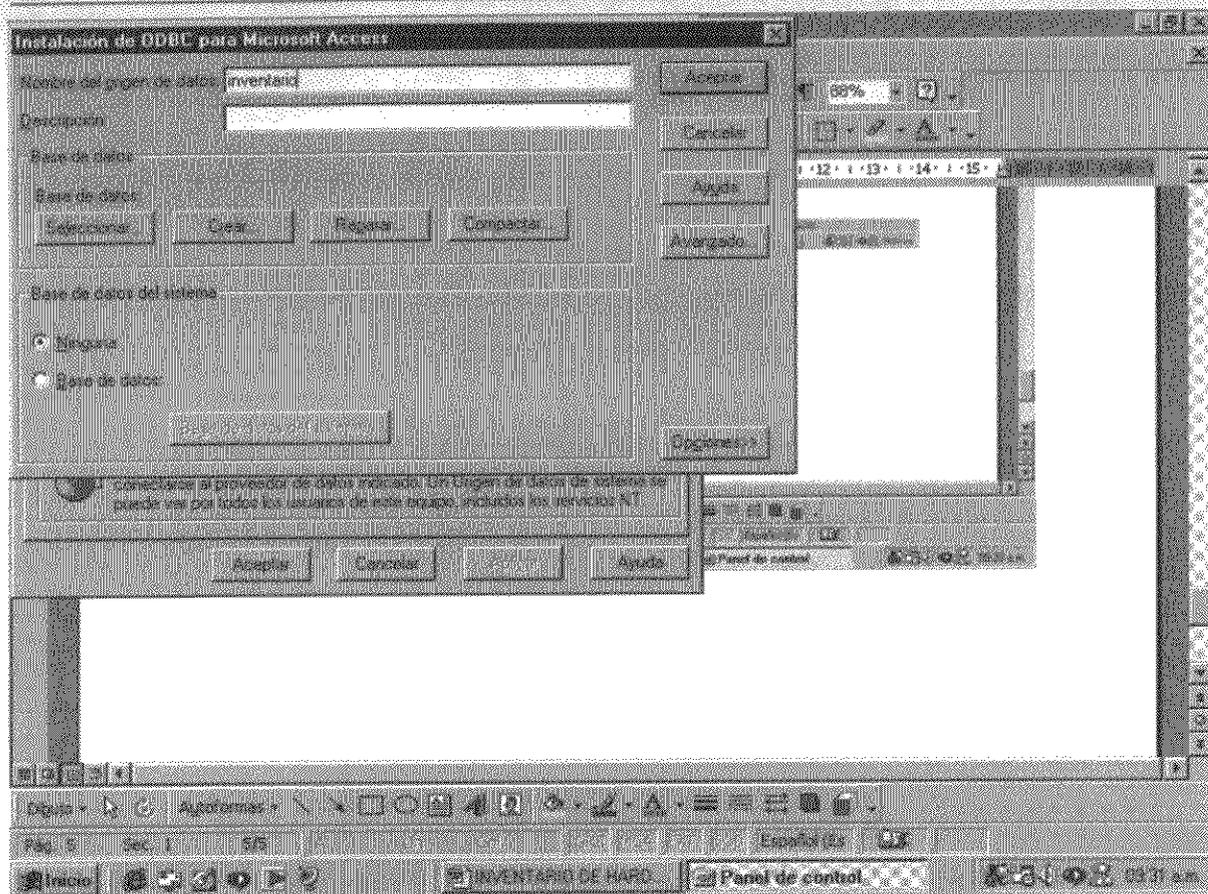
Haga clic en el botón Agregar y seleccione Microsoft Access Driver (\*.mdb)

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



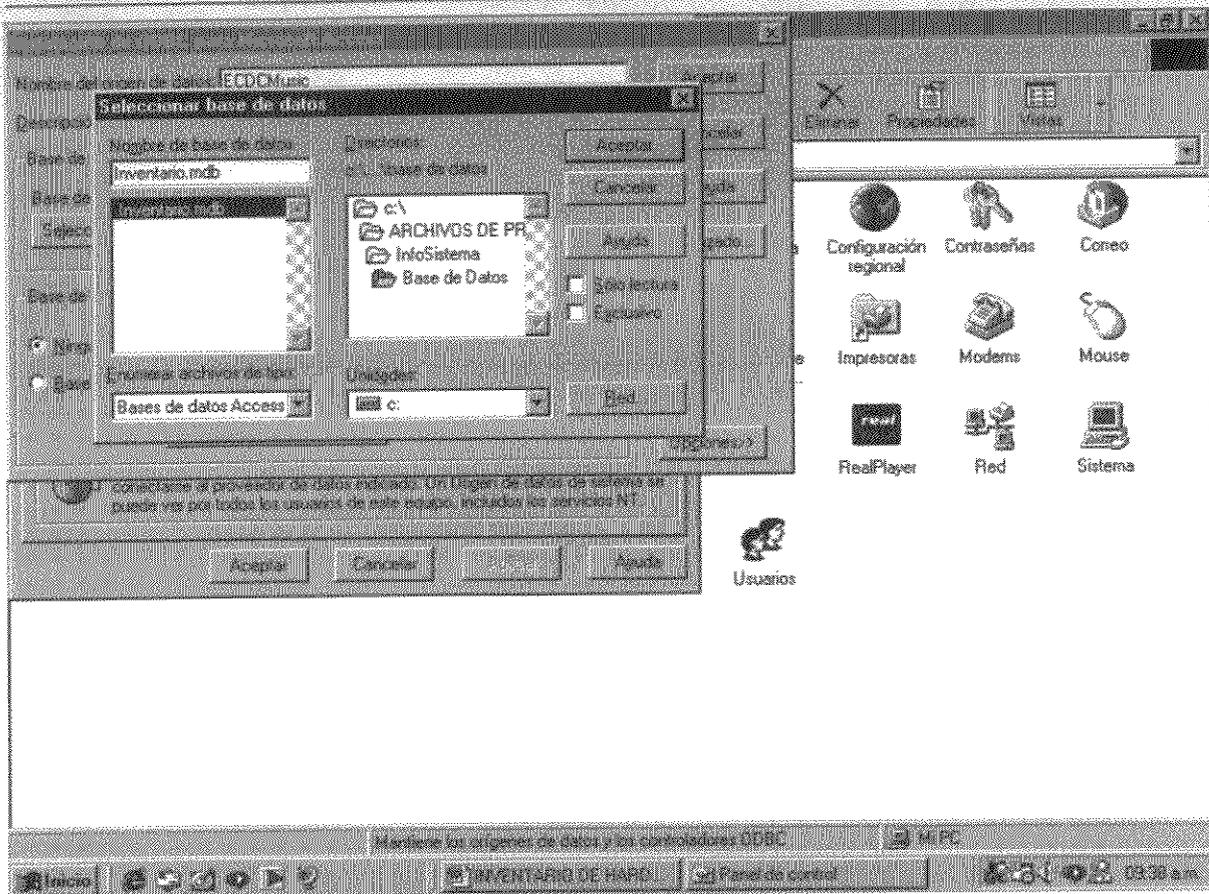
Colocar como nombre del origen de datos: inventario

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



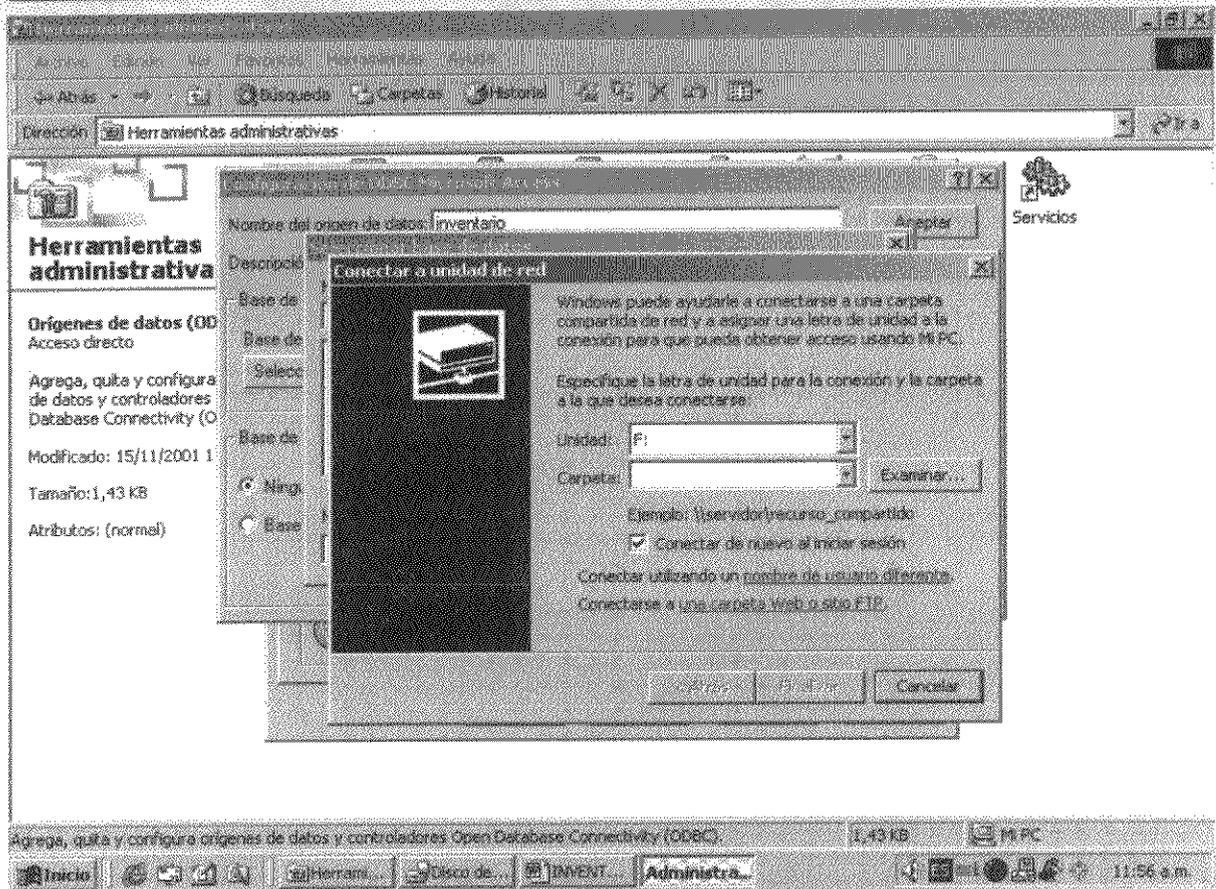
Haga clic en el botón Seleccionar del Marco Base de Datos, haga clic en el botón Red

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



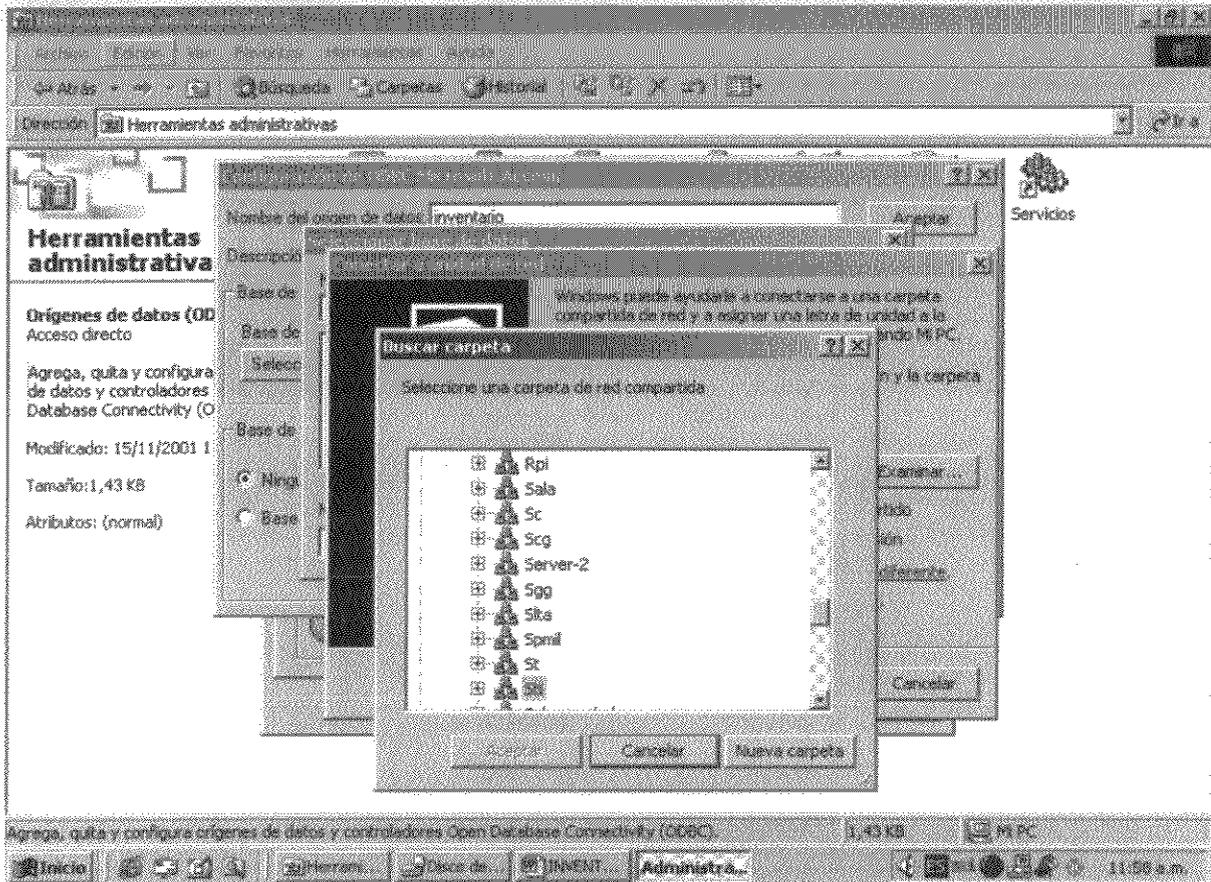
Haga clic en el botón examinar

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



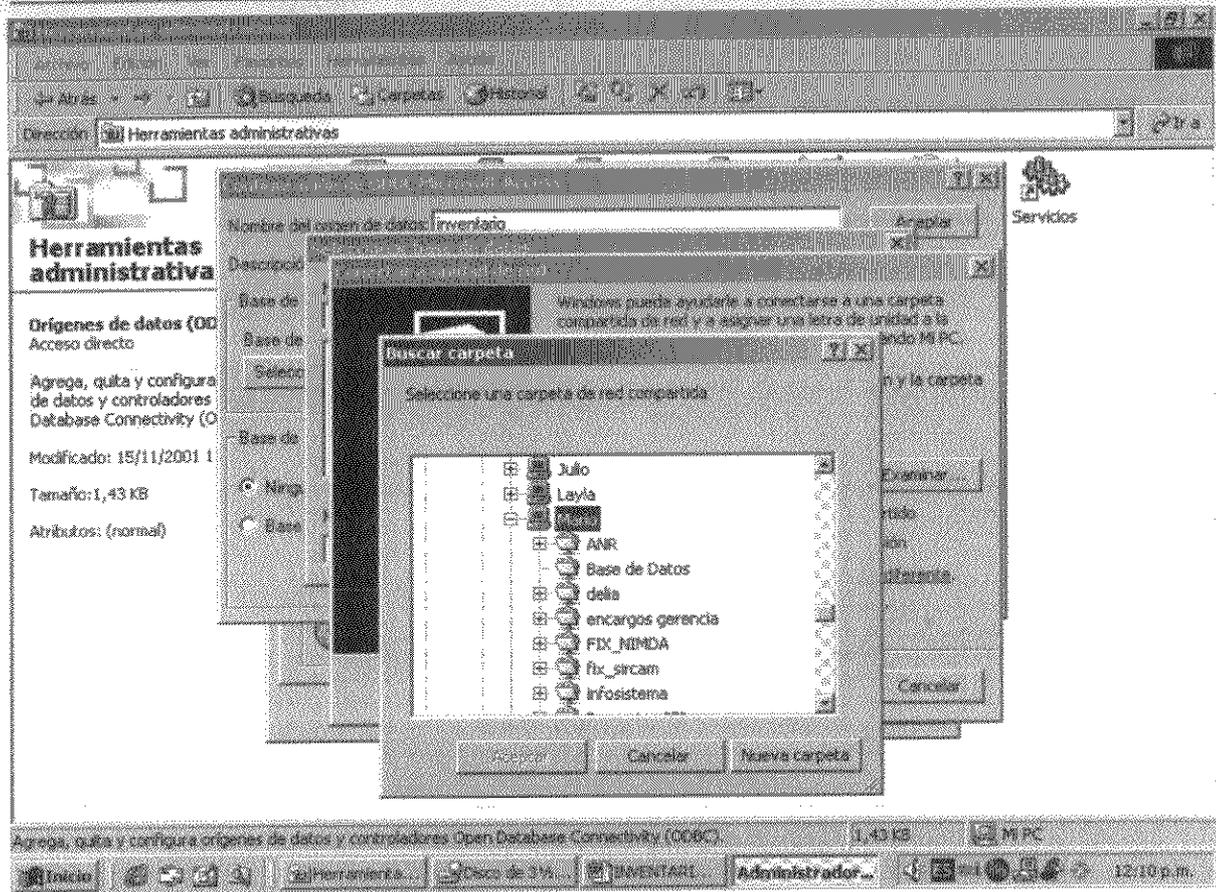
Seleccione el grupo de red al que pertenece por ejemplo STI

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



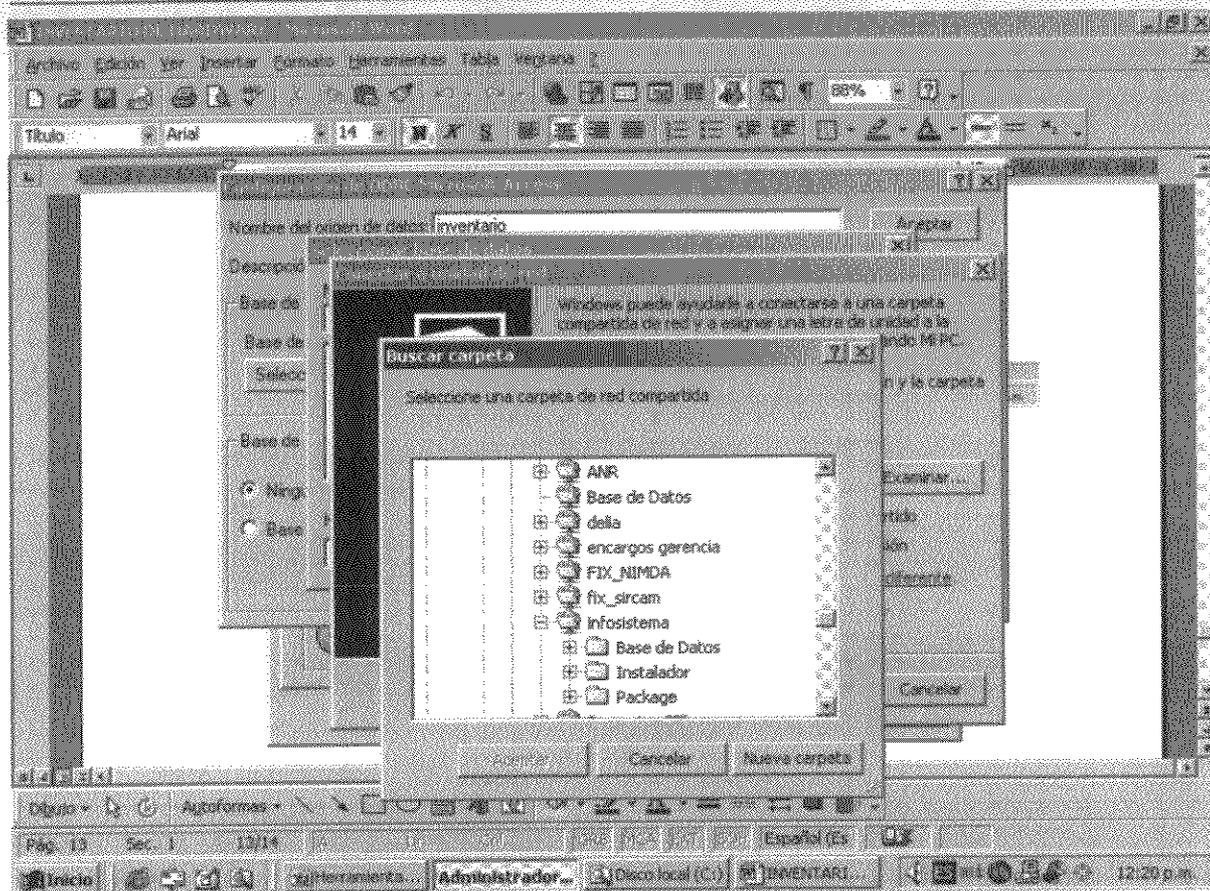
Seleccione la máquina donde se encuentra la Base de Datos y la Aplicación por ejemplo la máquina Mario

## SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



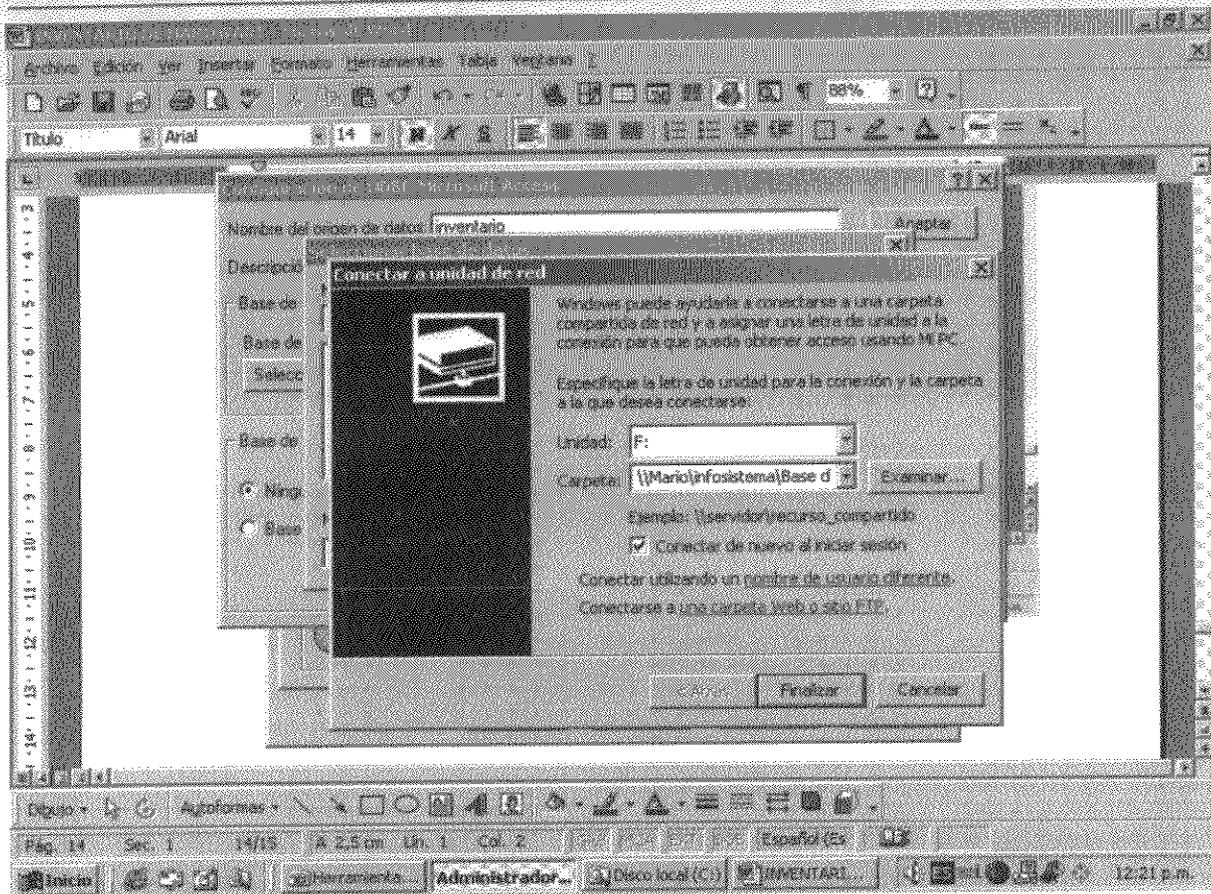
Haga clic en Infosistema y seleccione Base de Datos

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



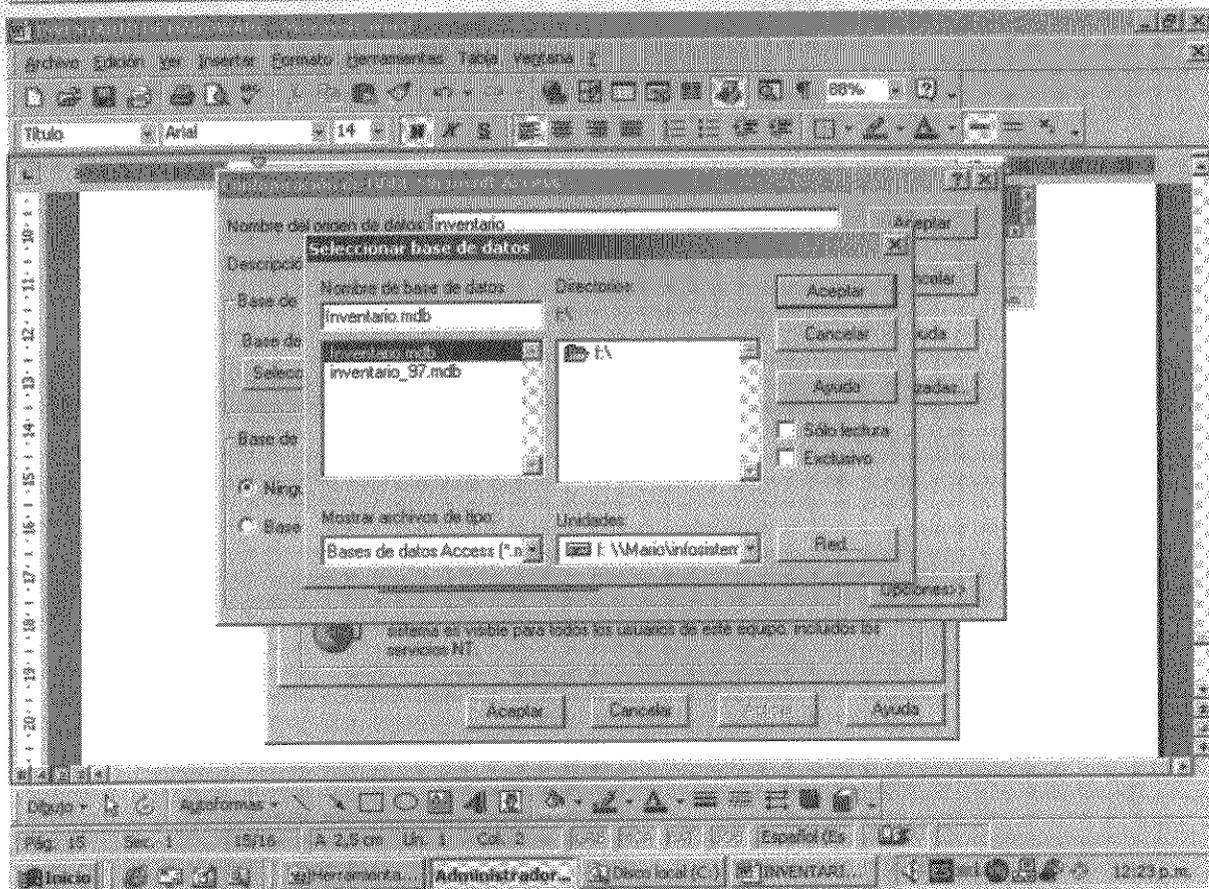
Haga clic en aceptar y luego haga clic en finalizar

## SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



Seleccione la Base de Datos INVENTARIO.MDB

### SOFTWARE PARA EL ALMACENAMIENTO DEL INVENTARIO



3. Por último acceder a Inicio y dentro de él acceder a Programas y dentro de éste buscar INFOSISTEMA y haga doble clic de INFOSISTEMA.

Una vez dentro del Sistema hacer clic en CARGA DE DATOS y Agregar la Información del Equipo con el cual se esta trabajando.

NOTA: en la primer máquina del Grupo de Red donde se está realizando el Inventario se deberá proceder de *FORMA MANUAL* y luego en las restantes máquinas que componen dicho GRUPO se procederá de *FORMA REMOTA*.

*Aldo H Polanco*  
Aldo Polanco

