INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

Normas de Seguridad para Afrontar el Virus I Love You

Lima, Mayo de 2000

Elaboración	:	Sub-Jefatura de Informática Impreso en los Talleres de la Oficina de Impresiones de la Oficina Técnica de Difusión Estadística y Tecnología Informática del Instituto Nacional de Estadística e Informática
Diagramación	:	Centro de Edición del INEI
Edición	:	500 Ejemplares
Domicilio	:	Av. Gral. Garzón Nº 658 Jesús María, Lima 11
Orden Nº	:	357 - OTDETI - INEI

Presentación

El Instituto Nacional de Estadística e Informática (INEI) en el marco del Plan de Acción diseñado para promover la seguridad de la información en las entidades públicas y privadas, pone a disposición el documento titulado NORMAS DE SEGURIDAD PARA AFRONTAR EL VIRUS “ILOVEYOU”.

Este virus que tardó solamente 5 horas para propagarse por cinco continentes a través de correo electrónico y, que afectó a un gran número de organismos nacionales e internacionales, en diversas partes del mundo, asombró a los expertos por su velocidad de propagación.

En el presente documento, se pretende proporcionar información y soluciones para afrontar y minimizar los efectos de este virus, particularmente peligroso por su capacidad de mutación.

En el primer capítulo se presentan definiciones y conceptos generales sobre los virus informáticos, su naturaleza, tipos y programas para contrarestarlos. En el segundo capítulo se describe y analiza el virus “ILOVEYOU”, como se manifiesta y propaga, cuales son los síntomas de infección y que daños causa, así como, los variantes o mutaciones del mismo.

En el tercer capítulo se presentan acciones de prevención, recomendaciones y prácticas para evitar la infección con este virus en particular. En el cuarto capítulo se tratan los procedimientos y acciones necesarios para afrontar y eliminar los efectos nocivos del virus cuando se verifica su incursión y propagación en los sistemas informáticos de la entidad.

En el quinto capítulo se presentan recomendaciones de políticas y normas de carácter general para la prevención, detección y eliminación de virus informáticos. Finalmente, en el capítulo sexto se presenta una lista de Páginas Web que contienen información sobre la materia.

El INEI, se complace en poner a disposición de las entidades de la Administración Pública y empresas del Sector Privado la presente publicación, como una contribución en las acciones orientadas a afrontar las amenazas del virus “ILOVEYOU”.

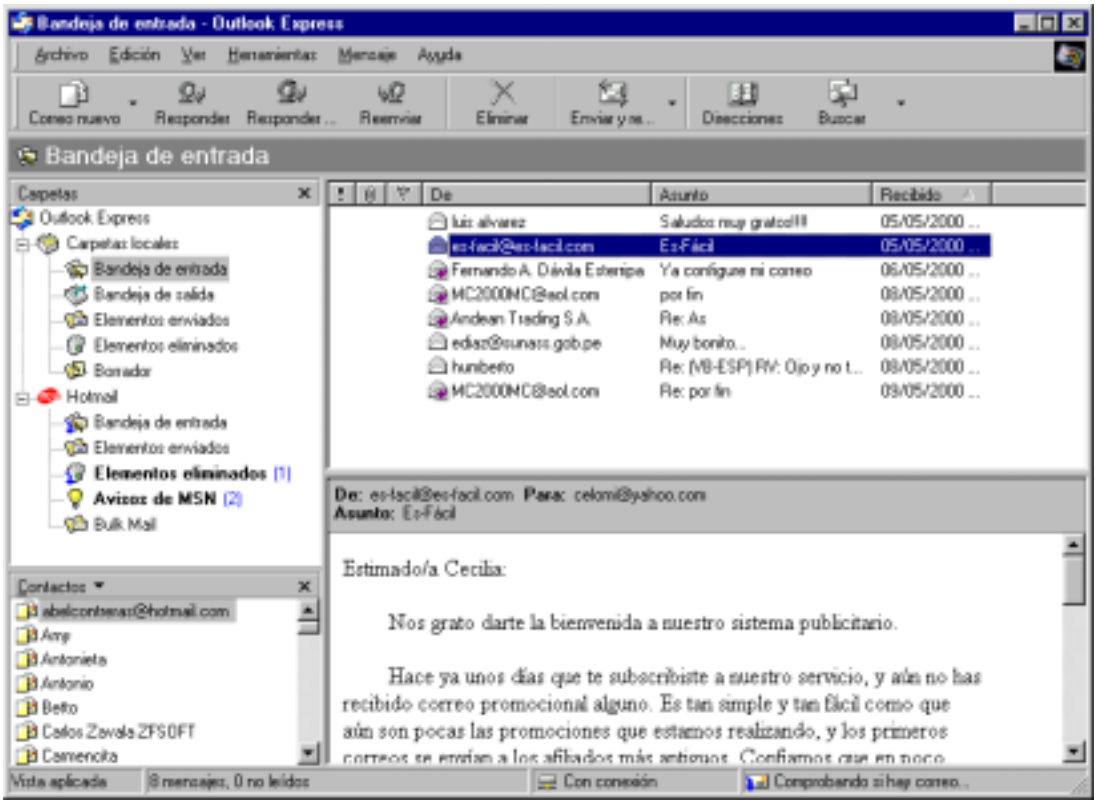
FELIX MURILLO ALFARO
JEFE
INSTITUTO NACIONAL DE
ESTADISTICA E INFORMATICA

Indice

Introducción

Cuando aún permanece en la memoria de muchos usuarios y administradores de red, las consecuencias del virus Melissa, la frase "I love you" se ha convertido en las últimas horas en la pesadilla de un inmenso número de servidores en el mundo. Las consecuencias han sido especialmente conocidas por usuarios y empresas que trabajan con Internet, utilizando el correo electrónico como herramienta de trabajo.

Los datos ofrecidos por agencias noticiosas a la fecha, informan que cientos de servidores en Estados Unidos, América Latina, Asia y Europa, han sufrido el ataque de un virus llamado "I Love You". Este virus informático es denominado técnicamente VBS/LoveLetter por agencias de seguridad de datos y las empresas proveedoreas de antivirus. Se activa sólo en el correo electrónico cliente de Microsoft Outlook. Una vez que se apertura el mensaje original infectado, inicia su actividad enviando en forma masiva mensajes iguales a las direcciones archivadas en la agenda de la aplicación outlook.



Esta nueva generación de virus resulta exponencialmente nociva, por tratarse de una actividad automática de spamming, o recepción no solicitada de mensajes de correo, hasta el punto de no necesitar de la activación del archivo incluido para el comienzo de la actividad. En el caso de “I Love You” sólo basta abrir el correo recibido.

Según las primeras investigaciones, el autor puede ser un adolescente filipino, cuyo lema proclamado ha sido "Odio ir a la escuela". De hecho el código fuente del mencionado virus incluye esta frase en su programación.

El Perú no es ajeno a los ataques del Virus “I LOVE YOU”. El INEI cuenta con información sobre ataques en algunas PCs de entidades públicas y noticias periodísticas, dan cuenta de estos ataques a entidades del sector privado.

“I LOVE YOU” representa la clarinada de alerta que la comunidad informática debe tomar en consideración, con el fin de disponer en el corto plazo una Política de Seguridad de Información y un conjunto de Programa de Seguridad y Contingencia específicos, que permitan proteger cada proceso institucional, potencialmente amenazado por esta nueva generación de virus informáticos.

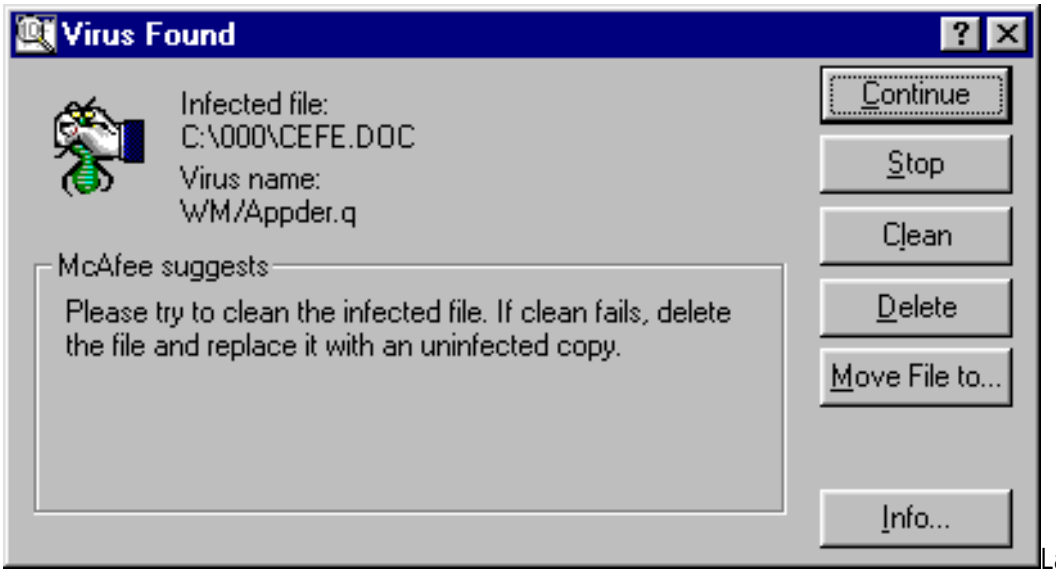
Esta publicación presenta información sobre el virus y desarrolla, en forma práctica, las medidas que los servicios informáticos de las entidades públicas y privadas deben poner en práctica para afrontar el virus “I Love You”.

I. Definiciones

¿QUE ES UN VIRUS INFORMATICO?

Los virus informáticos son programas que utilizan técnicas sofisticadas, diseñados por expertos programadores, que tienen la capacidad de reproducirse por sí mismos, unirse a otros programas, ejecutando acciones no solicitadas por el usuario. La mayoría de estas acciones son hechas con mala intención.

Los virus informáticos, atacan al usuario de una PC, destruyendo o afectando la información que no esté protegida. Actualmente los virus informáticos tienen diversos efectos.



La mayoría de los virus suelen ser programas residentes en memoria, se van copiando dentro de los archivos del computador.

VIRUS TIPO PROGRAMAS MALIGNOS

Son programas que deliberadamente borran archivos o software indicados por sus autores eliminándose así mismo cuando terminan de destruir la información.

Entre los principales programas malignos tenemos:

- Bombas Lógicas y de Tiempo
- Jokes
- Gusanos
- Caballos de Troya

- **Bombas Lógicas y de Tiempo**
  Se caracterizan por:

  - Son programas ocultos en la memoria del sistema, en el disco o en los archivos de programas ejecutables con extensión .COM y .EXE.
  - Una Bomba de Tiempo se activa en una fecha u hora determinada.
  - El daño que las bombas de tiempo puedan causar depende de su autor.
  - Una Bomba Lógica se activa al darse una condición específica.
  - Tanto las bombas lógicas como las bombas de tiempo, aparentan un mal funcionamiento del computador, hasta causar la pérdida de la información.

- **Jokes**

  Son bromas que semejan ser virus. Su objetivo es el de alarmar al usuario mediante bromas. Se caracterizan por:

  - Son programas desarrollados con el objetivo de hacer bromas, de mal gusto, ocasionando distracción y molestias a los usuarios.
  - Muestran en la pantalla mensajes extraños con la única intención de fastidiar al usuario.

- **Gusanos**

  Son programas cuya única finalidad es la de consumir la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta saturar la memoria RAM, Esta es su única acción maligna. Se caracterizan por:

  - Es un programa que se autoreproduce.
  - No infecta otros programas como lo haría un virus, pero crea copias de él, las cuales a su vez crean más copias.
  - Se usan mayormente para atacar grandes sistemas informáticos, mediante una red de comunicaciones como Intranet o Internet, donde el gusano creará más copias rápidamente, obstruyendo el sistema.

- Se propagan rápidamente en las computadoras.
- Utilizan gran cantidad de memoria del computador, disminuyendo la velocidad de ésta.

- **Caballos de Troya**

Son programas concretos que se introducen en el computador para instalarse en ellos. Emplean otras aplicaciones y abren una puerta a posibles acciones dañinas en el sistema. Se caracterizan por:

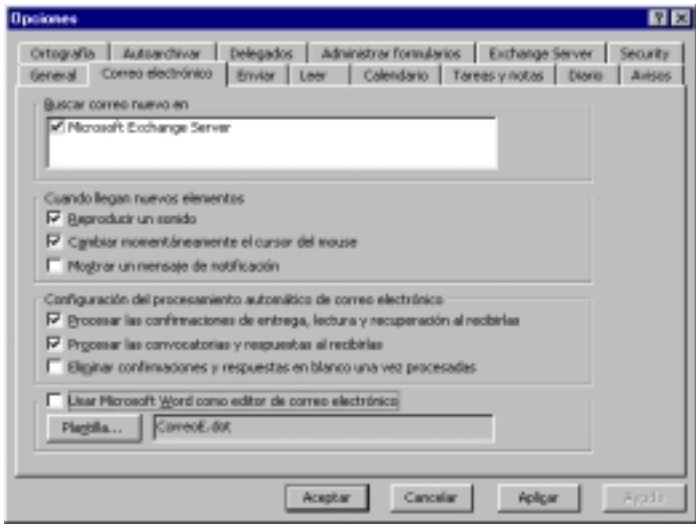
- Son programas que se introducen en el sistema bajo una apariencia totalmente diferente a la de su objetivo final.
- Se presentan como información perdida o basura sin ningún sentido.
- Al cabo de un determinado tiempo y esperando la indicación del programa, se activan y comienzan a ejecutarse.
- Sus autores lo introducen en los programas más utilizados o softwares ilegales como por ejemplo : Windows 95
- No se autoreproducen.
- Su misión es destruir toda la información que se encuentra en los discos.

VIRUS PARA CORREO ELECTRONICO

Este tipo de virus no puede copiarse ni tampoco destruye el disco duro del usuario con el hecho de leer un correo electrónico, ya que éstos se componen simplemente de texto.

El problema empieza cuando se ejecutan los archivos adjuntos ("attach mail"), ya que se puede recibir un archivo ejecutable que sí podría contener un virus. Por ello; es lo mejor no ejecutar directamente los archivos desde el mismo correo, sino almacenarlos en el disco duro y chequearlos con un antivirus antes de utilizarlos.

Si el programa de correo electrónico está configu-rado para leer los mensa-jes automáticamente con **Microsoft Word**, es posible recibir un virus de ma-cro e infectar el editor de textos **Word.** Cuando se tiene esta opción activada, se recomienda desactivar-la



(Herramientas /Opcio-nes) y antes chequear con un antivirus los archi-vos recibidos antes de ejecutarlos.

ANTIVIRUS INFORMATICOS

El antivirus es cualquier metodología, programa o sistema para prevenir la activación de los virus, su propagación y contagio dentro de un sistema y su inmediata eliminación y la reconstrucción de archivos o de áreas afectadas por los virus informáticos.

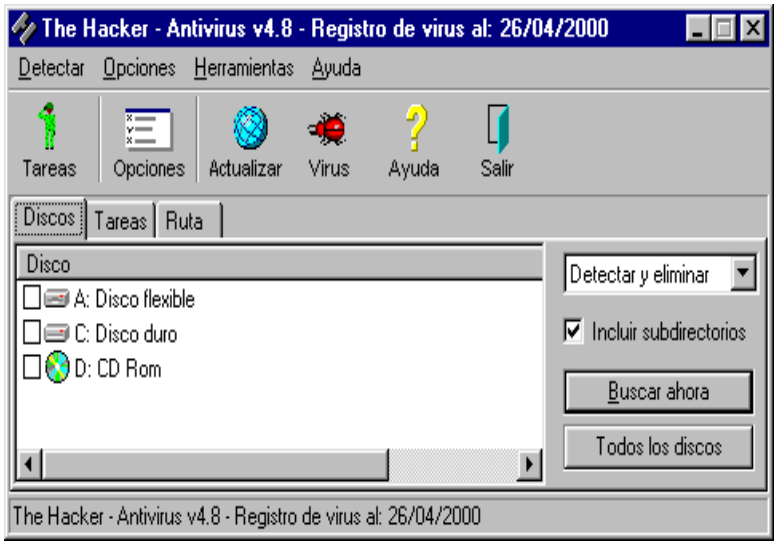
Los antivirus permiten la detección y eliminación de virus. Mediante una cadena del antivirus que busca, encuentra y elimina los distintos virus informáticos.

El software antivirus contrarresta de varias maneras los efectos de los virus informáticos al detectarlos. La mayoría de las soluciones se basan en tres componentes para la detección : exploración de acceso, exploración requerida, y suma de comprobación.

La exploración de acceso : Inicia automáticamente una exploración de virus, cuando se accede a un archivo, es decir al introducir un disco, copiar archivos, ejecutar un programa, etc.

La exploración requerida : El usuario inicia la exploración de virus. Las exploraciones se pueden ejecutar inmediatamente, en un directorio o volumen determinado.

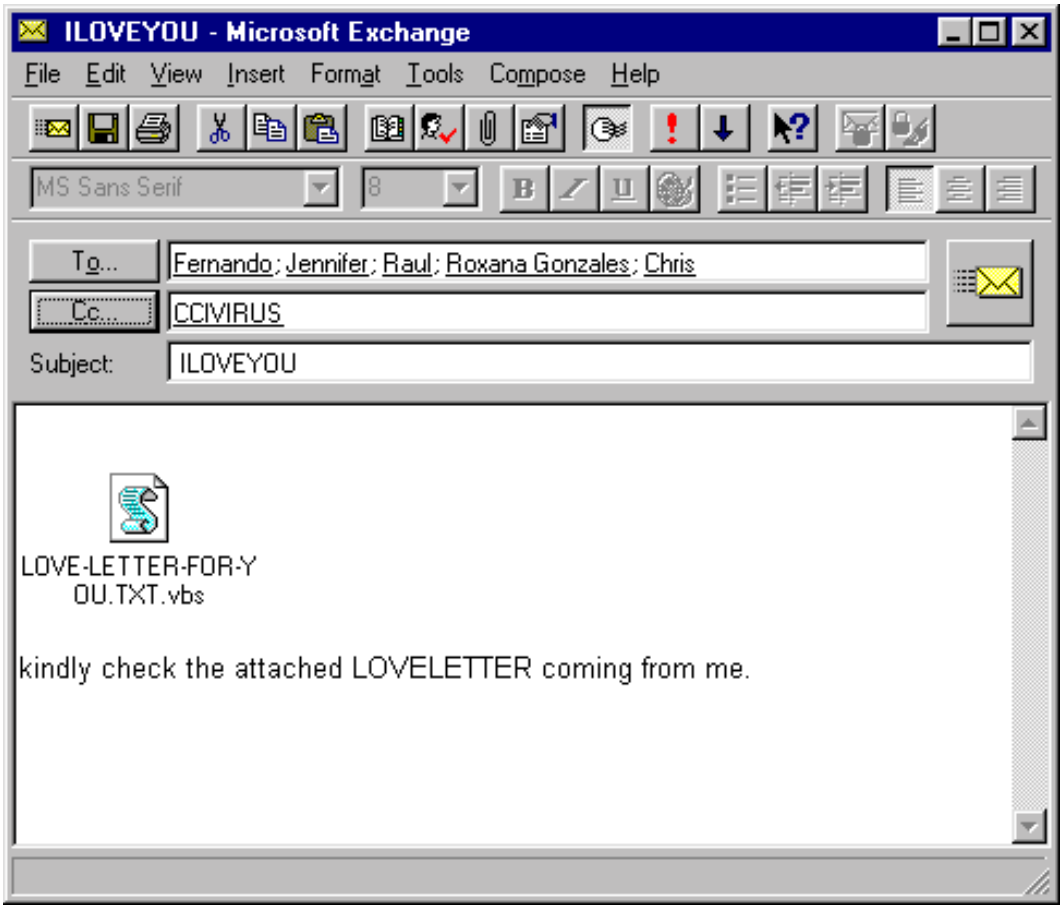
La suma de comprobación o comprobación de integridad : Método por el cual un producto antivirus determina si se ha modificado un archivo. Como el código vírico se une físicamente a otro archivo, se puede determinar tal modificación guardando la información del archivo antes de la infección.



La suma de comprobación es generalmente exacta y no necesita actualizaciones. Sin embargo la suma de comprobación no proporciona ni el nombre, ni el tipo de virus.

Los programas antivirus se componen fundamentalmente de dos partes : un programa que rastrea (SCAN) si en los dispositivos de almacenamiento se encuentra alojado algún virus y otro programa que desinfecta (CLEAN) a la computadora del virus detectado.

II. Virus “I Love You”



¿COMO SE PRESENTA?

Este virus se presenta bajo la modalidad de gusano. Está escrito en Visual Basic Script, y está infectando a miles de computadores a través del correo electrónico. Si recibe un mensaje con el asunto **"ILOVEYOU"** y el archivo adjunto **LOVE-LETTER-FOR-YOU.TXT.vbs**, le aconsejamos borrarlo inmediatamente.

Aunque la extensión VBS (Visual Basic Script) puede permanecer oculta en las configuraciones por defecto de Windows, lo cual puede hacer pensar que se trate de un inocente archivo de texto.

Cuando se abre el archivo infectado, el virus gusano procede a infectar el sistema y expandirse rápidamente, enviándose a todos aquellos contactos que tiene la agenda de

direcciones, incluidas las agendas globales corporativas. Es importante no ejecutar ningún archivo adjunto que venga con dicho mensaje.

Un análisis preliminar permite identificar, a partir de las primeras líneas, el código del virus gusano que procede de Manila, Filipinas, y el autor se apoda **"spyder".** Sin embargo, esta información está siendo investigada:

rem barok -loveletter(vbe) < i hate go to school >
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines

¿COMO SE INSTALA EL VIRUS?

El virus VBS/LoveLetter.A llega en un mensaje de e-mail similar a:

Asunto: ILOVEYOU
Cuerpo del mensaje: kindly check the attached LOVELETTER coming from me..
Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

Si el usuario abre el archivo adjunto (LOVE-LETTER-FOR-YOU.TXT.vbs), el gusano se copia a los siguientes directorios:

\windows\system -> MSKernel32.vbs
\windows -> Win32DLL.vbs
\windows\system -> LOVE-LETTER-FOR-YOU.TXT.vbs

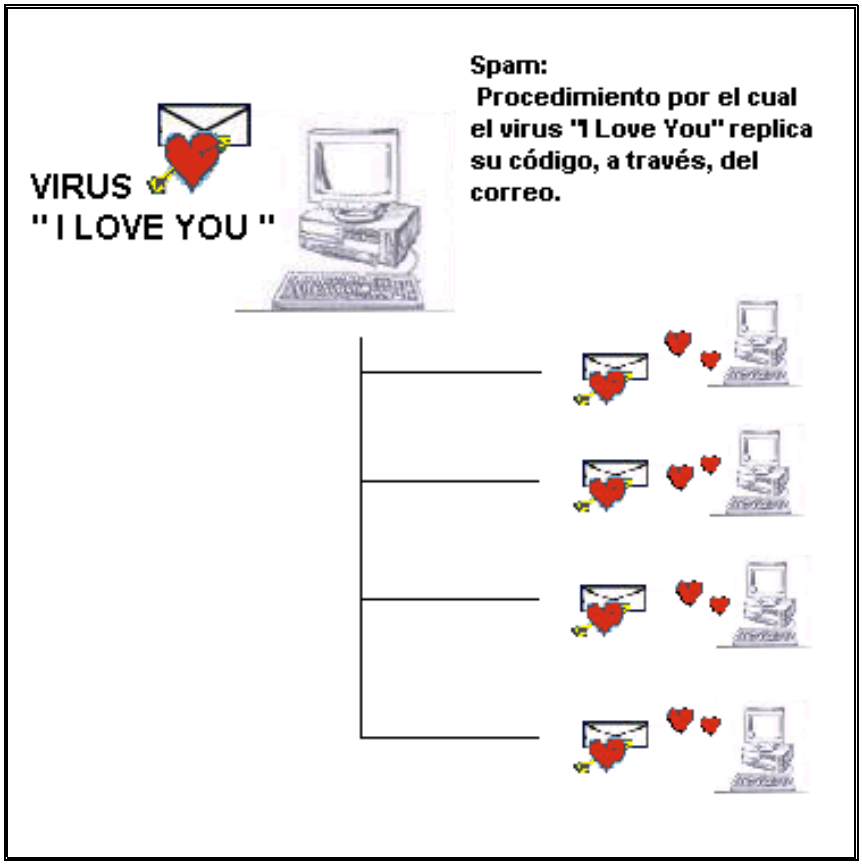
Después de esto modifica el registro de Windows para ejecutarse automáticamente en cada inicio del sistema (archivos MSKernel32.vbs y Win32DLL.vbs):

Registro:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"MSKernel32" = "{\windows}\systemMSKernel32.vbs"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
"Win32DLL" = "{\windows}\Win32DLL.vbs"

MAILS EN MASA:

El siguiente paso del virus gusano es enviar por e-mail a todos los usuarios de la libreta de direcciones del OutLook. El virus gusano genera múltiples mensajes del tipo:

> ***Asunto: ILOVEYOU***
> ***Cuerpo del mensaje: kindly check the attached LOVELETTER coming from me..***
> ***Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs***



¿CUÁLES SON LOS SINTOMAS DEL VIRUS?

1. La recepción de un mensaje de correo electrónico que presenta las siguientes características:

   - En el Asunto puede leerse alguno de los siguientes textos: ILOVEYOU
     - Susitikim shi vakara kavos puodukui....
     - fwd: Joke
     - Mothers Day Order Confirmation
     - Dangerous Virus Warning
     - Virus ALERT!!!
     - Important ! Read carefully !!

   - La existencia de un archivo adjunto cuyo nombre puede ser:
     - LOVE-LETTER-FOR-YOU.TXT.vbs
     - VERY FUNNY.VBS.
     - MOTHERSDAY.vbs
     - VIRUS_WARNING.JPG.VBS
     - PROTECT.VBS
     - IMPORTANT.TXT.vbs

2. Si al recibir el mensaje, el usuario lo abre, el equipo resultará infectado. Los síntomas de la infección son, entre otros:

   Cambios en los archivos con extensión :vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, wav, txt, gif, doc, htm, html, xls, com, bat, mp3 y mp2 .

3. La aparición, en el registro de configuración de Windows, de las siguientes entradas:

   - HKEY_LOCAL_MACHINE\Software\MicrosoftWindows\CurrentVersion\ Run\MSKerne32
   - HKEY_LOCAL_MACHINE\Software\MicrosoftWindows\ CurrentVersion\Run\Services\Win32DLL
   - En la variante "I" los archivos MSKernel32.vbs y Win32DLL.vbs, se llaman ESKernel32.vbs y ES32DLL.vbs, respectivamente.

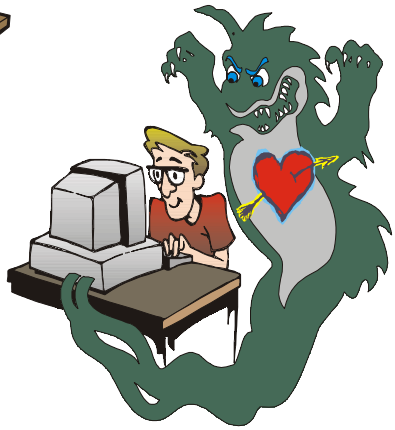
Forma de Ingreso y los estragos del Virus ”I Love You”

Un correo inhabitual y redactado en inglés
Llega al buzón electrónico de la computadora

1

Tema: “ILOVEYOU”
Mensaje: “abra el archivo adjunto donde se encuentra mi carta de amor”
Archivo adjunto: “LOVE-LETTER-FOR-YOU.TXT-vbs”

2



La apertura del archivo adjunto “LOVE-LETTER-FOR-YOU.TXT.vbs” Activa el virus

3

El virus puede...

- Introducirse en cada ordenador de una red
- Corromper los archivos al insertar el virus

-Enviar por sí mismo mensajes trampa a los destinatarios que figuran en la agenda de direcciones

Penetrar en el sistema de exploración Y destrozar los archivos

-Apoderarse de las contraseñas de acceso a internet
- Multiplicarse

Entre los archivos amenazados, aquellos que tienen como extensión:

.JPG	*.VBE*	*.JS*	*.JSE*
.JPEG	*.CSS*	*.SCT*	*.Mp3*
.VBS	*.WSH*	*.HTA*	*.Mp2*

¿QUE DAÑOS CAUSA EL VIRUS?

El virus sobrescribe con su código maligno los archivos con extensiones:

- .VBS y .VBE.

Elimina los archivos con extensiones:

- .JS, .JSE, .CSS, .WSH, .SCT y .HTA,

y crea otros archivos con el mismo nombre y extensión .VBS en el que introduce su código maligno.

También localiza los archivos con extensión:

- .JPG, .JPEG, .MP3 y .MP2, eliminandolos del disco duro,

y crea otros archivos, donde el nuevo nombre está formado por el nombre y la extensión anterior más la extensión .VBS.

A continuación presentamos los tipos de archivos que son afectados por el virus "I Love You":

EXTENSIÓN	ARCHIVOS
.VBS	Visual Basic Script
.VBE	Utilitario de gráficos del Script – Gráficos 3D
.JS	Java Script
.JSE	Java Script
.CSS	Hojas de Estilo (Cascade Style Sheet)
.WSH	Windows Scripting Host
.SCT	Componente (Windows Script Componet)
.HTA	Componente (Windows Script Componet)
.JPG	Gráfico
.JPGE	Gráfico
.MP3	Música
.MP2	Música

VARIANTES DEL VIRUS “I LOVE YOU”

Se han detectado múltiples variantes del virus “I Love You”. Entre ellas se tiene:

- **VBS/LoveLetter.B, alias “Lithuania”.**

  Diferencias:

  Asunto : "Susitikim shi vakara kavos puodukui...".
  Cuerpo del mensaje: kindly check the attached LOVELETTER coming from me.

- **VBS/LoveLetter.C, alias "Very Funny".**

  Diferencias:

  Asunto: "fwd: joke"
  Archivo adjunto: VERY FUNNY.VBS.
  Cuando se envía a través de un canal de IRC, el archivo recibe el nombre VERY FUNNY.HTM.

- **VBS/LoveLetter.D, alias “BugFix”**

  Diferencias:

  Asunto: ILOVEYOU
  Archivo adjunto: LOVE-LETTER-FOR-YOU.TXT.vbs
  Cuerpo del mensaje: kindly check the attached LOVELETTER coming from me.
  Nota: en el registro de Windows: WIN- -BUGSFIX.exe en vez de WIN-BUGSFIX.exe

- **VBS.LoveLetter.E (alias "Mother's Day")**
  Diferencias:

  Asunto: Mothers Day Order Confirmation
  Fichero adjunto: mothersday.vbs
  Cuerpo del mensaje: We have proceeded to charge your credit card for the amount of $326.92 for the mothers day diamond special. We have attached a detailed invoice to this email. Please print out the attachment and keep it in a safe place.Thanks Again and Have a Happy Mothers Day! mothersday@subdimension.com

Nota: mothersday.HTM enviado por IRC. Comentario en el código: rem hackers.com, & start up page to hackes.com, l0pht.com, or 2600.com

- **VBS/LoveLetter.F, alias “Virus Warnig”**

  Diferencias:

  Asunto: "Dangerous Virus Warning"
  Archivo adjunto: VIRUS_WARNING.JPG.VBS.
  Cuando se envía a través de un canal de IRC, el archivo recibe el nombre de:

- **URGENT_VIRUS_WARNING.HTM.**
  Cuerpo: "There ia a dangerous virus circulating. Please click attached picture to view it and learn to avoid it"
  1. Las direcciones web a las que intenta conectarse son:
     - HKCU\Software\Microsoft\Internet Explorer\Main\Start Page, con el valor
     - http://www.skycable.tucows.com/files2/setup24.exe
     - HKCU\Software\Microsoft\Internet Explorer\Main\Start Page, con el valor http://www.skycable.tucows.com/files2/setup24.exe
     - HKCU\Software\Microsoft\Internet Explorer\Main\Start Page, con el valor http://www.skycable.tucows.com/files2/setup24.exe
     - HKCU\Software\Microsoft\Internet Explorer\Main\Start Page, con el valor http://www.skycable.tucows.com/files2/setup24.exe

  En ninguna de dichas direcciones se han encontrado instrucciones para descargar algún archivo infectado.

  2. También actúa sobre los archivos con extensiones: WAV, TXT, GIF, DOC, HTM, HTML y XLS.

- **VBS/LoveLetter.G, alias “Virus Alert”**

  Diferencias:

  1. El mensaje de correo electrónico en el que se envía tiene las siguientes características, en inglés:

     De: support@symantec.com
     Asunto: "Virus ALERT!!!"

Cuerpo: "Symantec's AntiVirus Research Center began receiving reports regarding VBS.LoveLetter.A virus early morning on May 4, 2000 GMT. This worm appears to originate from the Asia Pacific region.

Distribution of the virus is widespread and hundreds of thousands of machines are reported infected.

The VBS.LoveLetter.A is an Internet worm that uses Microsoft Outlook to e-mail itself as an attachment.

The subject line of the e-mail reads ILOVEYOU, with the attachment titled LOVE-LETTER-FOR-YOU.TXT.VBS. Once the attachment is opened, the virus replicates and sends an e-mail to all e-mail addresses listed in the address book. The virus also spreads itself via Internet relay chat and infects files on local and remote drives including files with extensions vbs, vbe, js, sje, css, wsh, sct, hta, jpg, jpeg, mp3, mp2. Users should exercise caution when opening e-mails with this subject line, even if the e-mail is from someone they know, as that is how the virus is spread.

Symantec Corp. today announced availability of the virus definition to detect, repair and protect users against the VBS.LoveLetter.A virus. This definition is available now via Symantec's LiveUpdate and can also be downloaded from the following web sites:
http://www.symantecstore.com/AF74211/promo/
loveletter
http://www.digitalriver.com/symantec

Also as a quick solution Symantec Corp. offers Visual Basic Script to protect your PC against this worm. (See attached.) Note! When executed, this script will protect Your PC from being INFECTED by BS.LoveLetter.A virus. To cure already infected PC's download Norton Antivirus Updates mentioned above.
Symantec Corporation - a world leader in internet security technology."

2. El archivo incluido en el mensaje de correo electrónico en el que se envía se denomina:

   - **PROTECT.VBS.**
     Cuando se envía a través de un canal de mIRC, el archivo recibe el nombre de:

   - **PROTECT.HTM.**

3. Las direcciones web a las que intenta conectarse son:

   - HKCU\Software\Microsoft\Internet Explorer\Main\Start Page, con el valor http://3doc.dailypussy.com/gallery/bunny.html
   - HKLM\Software\Microsoft\Internet Explorer\Main\Start Page, con el valor http://3doc.dailypussy.com/gallery/bunny.html
   - HKLM\Software\Microsoft\Internet Explorer\Main\Search Page, con el valor http://astalavista.box.sk
   - HKLM\Software\Microsoft\Internet Explorer\Main\Search Page, con el valor http://astalavista.box.sk
   - HKLM\Software\Microsoft\Internet Explorer\Main\Defaul_Page_URL, con el valor http://www.persiankitty.com
   - HKLM\Software\Microsoft\Internet Explorer\Main\Local Page, asignándole el valor PROTECT.HTM, que es el archivo que ha copiado en el directorio SYSTEM de Windows.

   En ninguna de dichas direcciones se han encontrado instrucciones para descargar algún archivo infectado.

4. También actúa sobre los archivos con extensiones: COM y BAT

- **VBS/LoveLetter.H, alias “No Comments”**

  Diferencia:
  Asunto: ILOVEYOU
  Archivo adjunto: LOVE-LETTER-FOR-YOU.TXT.vbs
  Cuerpo del mensaje: kindly check the attached LOVELETTER coming from me.
  Nota: las líneas de comentario han sido eliminadas.

- **VBS.LoveLetter.I, alias "Important! Read carefully!!"**

  Diferencia:
  Asunto: Important! Read carefully!!
  Archivo adjunto: Important.TXT.vbs
  Cuerpo del mensaje: Check the attached IMPORTANT coming from me!
  Notas: línea de comentario: by: BrainStorm / @ElectronicSouls. También copia los archivos ESKernel32.vbs y ES32DLL.vbs, y añade comentarios al script.ini de mIRC referentes a BrainStorm y ElectronicSouls, así como envía el archivo IMPORTANT.HTM a través de DCC.

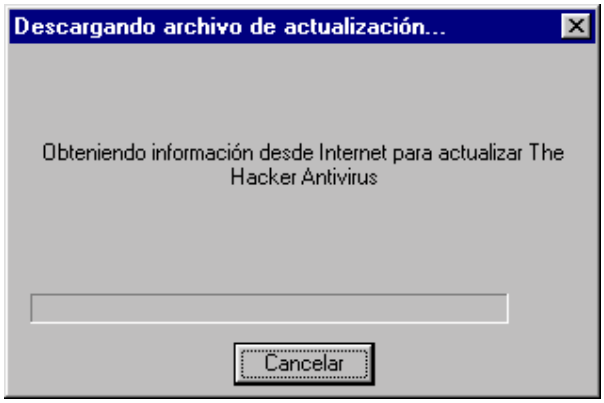
III. Prevención

¿QUE HACER ANTES DE SER INFECTADO?

Para hacer frente al virus “I LOVE YOU” y a todo tipo de códigos malignos es esencial:

- Instalar un antivirus eficaz en su PC o red.
- Actualizar dicho antivirus constantemente, ya que los virus pueden surgir de la nada y propagarse de manera exponencial en cuestión de horas.
- No ejecutar ningún archivo adjunto a un mensaje de correo que provenga de una fuente desconocida y aquellos que, aun proviniendo de fuentes conocidas, no hayan sido solicitados
- Infórmese puntualmente sobre todos las novedades en la seguridad informática

Actualización permanente del software antivirus



IV. Eliminación

¿QUE HACER SI ESTA INFECTADO?

En caso no cuente con un antivirus actualizado se recomienda llevar adelante el siguiente procedimiento para eliminar el virus:

El virus gusano crea las siguientes claves en el registro (regedit), que deberán ser borradas para evitar que el virus se ejecute de forma automática al iniciar el sistema:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32 DLL

También será necesario borrar los archivos:

- WIN32DLL.VBS
  ubicado en el directorio de Windows (por defecto \WINDOWS)

- MSKERNEL32.VBS
- LOVE-LETTER-FOR-YOU.VBS
  ubicados en el directorio de sistema (por defecto \WINDOWS\SYSTEM)

Si el virus realizó lo anterior es necesario revisar si se activó la segunda parte del código maligno del virus gusano, que es modificar la página de inicio de Internet Explorer con una de las 4 direcciones, que elige según un número aleatorio bajo el dominio http://www.skyinet.net. Estas direcciones apuntan al archivo WIN-BUGSFIX.EXE, y una vez descargado modifica el registro de Windows para que este programa también sea ejecutado cuando se inicia el sistema modificando la configuración de Internet Explorer, presentando en esta ocasión una página en blanco como inicio.

Si el virus gusano ha conseguido realizar el paso anterior también se deben borrar los archivos el archivos:

- WIN-BUGSFIX.EXE, ubicado en el directorio de descarga de Internet Explorer y la entrada del registro:
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
  CurrentVersion\Run\WIN-BUGSFIX

El virus gusano también detecta la presencia del programa mIRC, buscando algunos de los siguientes archivos:

- mirc32.exe,
- mlink32.exe,
- /mirc.ini y
- script.ini.

En caso de que se encuentren en el sistema el virus gusano escribe en el mismo directorio su propio archivo SCRIPT.INI donde podemos encontrar, entre otras líneas, las siguientes instrucciones:

```
n0=on 1:JOIN:#:{
n1=  /if ( $nick = = $me ) { halt }
n2=  /.dcc send $nick "&dirsystem&"\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

V. Recomendaciones

POLITICAS DE SEGURIDAD ANTE LOS VIRUS

Como parte de la política de seguridad de información institucional, se debe poner en marcha una política de seguridad ante los virus.

La política de seguridad se comprueba realizando el seguimiento de las medidas diseñadas, mediante la implementación de auditorías permanentes, que permiten asegurar que la política se adapta a la organización.

El desarrollo de redes globales a las que se accede desde cualquier parte del mundo con un coste bajo y desde cualquier hogar como es INTERNET, aumenta estadísticamente la probabilidad de que alguien no autorizado intente acceder a la red de la institución.

Las políticas de seguridad deben considerar la tipología de la información, los usuarios de la misma y de los equipos y sistemas.

Una política de seguridad debe contemplar:

- Seguridad física de los locales y acceso donde se encuentran los sistemas.
- Asegurarse contra todos los riesgos posibles. Esto requiere un periodo de observación y una clasificación de los recursos y sistemas que están en la organización, los que están fuera, los puntos de acceso remoto, las costumbres y hábitos del personal.
- Asegúrese que es una integración por encima de los sistemas, plataformas y elementos que constituyen las redes.
- La gestión de la seguridad debe de ser centralizada.

La política de seguridad debe especificar las tareas a realizar, sus responsables, cómo se definen los niveles de acceso, cómo se auditan los planes operativos, cómo se realizará el seguimiento, dónde deben ponerse en marcha medidas específicas (firewall o cortafuegos, filtros, control de acceso, antivirus corporativos, entre otros), el plan de capacitación del personal de la organización.

RIESGOS POTENCIALES

Los riesgos potenciales se pueden presentar por:

- Modificación ilegal de los programas (virus, caballos de troya, gusanos).
- Destrucción y modificación de la información de la institución.
- Cambiar la secuencia de los mensajes.
- Pérdida del anonimato o de la confidencialidad.
- Uso de una identidad falsa para hacer transacciones o enviar operaciones.
- Impedir que un usuario que no puede usar los recursos lo haga.
- Violación de los sistemas de control de acceso.

MECANISMOS PARA GARANTIZAR LA SEGURIDAD

La política de seguridad debe contemplar mecanismos, que garanticen la seguridad en una organización. Como consecuencia de ello no existen políticas aisladas, sino políticas que integran planes y programas de seguridad para toda la institución, incluyendo a la seguridad informática. Estos son:

- **Administración de passwords o claves de acceso:** Este componente es uno de los puntos más vulnerables para atacar los sistemas de una organización. Es necesario disponer de planes que aseguren la confidencialidad, la protección, identificación de los passwords que han sido descubiertos y su renovación permanente, para evitar que personas ajenas a la institución tengan acceso a los sistemas.

- **Gestión criptografía o cifrado de mensajes y datos:** Permite proteger a la institución de los espías pasivos que son, por otra parte, los más difíciles de detectar ya que sólo son observadores de lo que pasa en la organización, sin modificar la información ni los procesos en los que intervienen.

- **Administración de Respaldo o Copias de Seguridad:** Es necesario disponer de planes y procedimientos documentados, para realizar copias de seguridad de la información, es importante que se incorporen conceptos como:

    - Sistemas de backup para redes, que incorporan funciones de softwares independientes del hardware sobre el que se realizan copias.
    - Automatización de los procesos de backup, evitando la intervención manual.
    - Administración de estándares que permitan operar las funciones de archivos y backups sobre distintas redes y plataformas.

- Gestión de archivos jerárquicos que permitan a los usuarios trabajar con archivos que están guardados en librerías o en sistemas off-line.

Dichos conceptos deben ser manejados y gestionados en forma centralizada.

- **Planificación de Desastres**
  Los planes de seguridad deben incluir una planificación de desastres de todo tipo (desastres naturales, ataques, sabotajes, entre otros). Para lo cual la organización debe tomar medidas que aseguren que la información institucional no se vea afectada.

- **Medidas Antivirus**
  La instalación de un sistema de programas antivirus y procedimientos es la medida más empleada por las empresas para protegerse de ataques virales.

- **Control de Acceso,** se puede realizar con sistemas que combinan hardware y software. Una opción utilizada habitualmente son sistemas (módem, software, tarjetas antivirus, etc.) que generan una llamada a un puesto o teléfono de control preprogramado, que devuelve al punto de acceso la ID a comprobar.

  Los sistemas más sofisticados incluyen lectores de tarjetas de crédito, tarjetas inteligentes, detectores de huella digital o simplemente generadores de clave que son únicas para cada sesión.

- Firewalls o Cortafuegos
  Los cortafuegos o "firewalls" son mecanismos que permiten filtrar los accesos permitiendo aislar en función de diferentes criterios o parámetros, establecen quienes pueden y quienes no puede entrar en un sistema.

  Los cortafuegos se pueden instalar en los routers, en los servidores o en máquinas aisladas cuya única función es analizar y filtrar lo que puede y no puede acceder de dentro afuera y viceversa. Algunos de ellos disponen de facilidades que les permiten identificar y cerrar el acceso a virus o programas extraños.

NORMAS PARA LA PREVENCION, DETECCION Y ELIMINACION DE VIRUS INFORMATICO

La Directiva Nro. 016-94-INEI/SJI, “Normas para la prevención, detección y eliminación de virus informático en los equipos de cómputo de la Administración Pública” contiene los siguientes procedimientos:

Del Control de la Información Ingresada, que en los artículos 5.1 al 5.5 y del 6.1 al 6.15 se estipula:

5.1 No deben utilizarse diskettes usados provenientes del exterior de la institución.

5.2 Si por razones de trabajo fuera necesario la utilización de un medio magnético u óptico venido del exterior, éste deberá necesariamente pasar por los controles siguientes:

- **a.** Identificar el medio de almacenamiento que contiene la información. Los medios magnéticos u ópticos de almacenamiento (diskettes, cintas, cartuchos, discos u otros) que contienen archivos de información, deben estar debidamente etiquetados, tanto interna como externamente.
- **b.** Chequear el medio magnético u óptico, mediante un procedimiento de detección de virus, establecido por el organismo competente de la Institución.
- **c.** Registrar el medio magnético u óptico, su origen y la persona que lo portó.

5.3 Los medios de detección de virus deben ser actualizados mensualmente, de acuerdo a las nuevas versiones de los detectores de virus que adquiera la Institución. Deberán utilizarse programas antivirus originales.

Del Personal usuario de las Computadoras

5.4 El personal que tiene acceso a las computadoras en forma monosuaria, deberá encargarse de detectar y eliminar en los medios magnéticos u ópticos, la infección o contagio con virus. A tal efecto, utilizará los procedimientos establecidos por el órgano competente de la Institución. Este personal es responsable del control de los medios magnéticos u ópticos venidos del exterior, así como de la posible introducción de virus en el equipo de cómputo.

5.5 Las computadoras conectadas a una Red, preferentemente, no deberán tener unidades de diskettes a fin de prevenir la infección de virus informático. El uso de los diskettes deberán ser efectuados por el administrador de la red.

Otras Medidas de Prevención Contra Virus

6.1 Semanalmente deberá efectuarse un respaldo de toda la información útil que se encuentra almacenada en el disco duro. Dicha actividad será realizada por el designado para este fin.

6.2 En caso de que se labore en red o en modo multiusuario, el administrador de la red hará un respaldo diario de la información útil del disco duro.

6.3 Por ningún motivo debe usarse los servidores de red como estaciones de trabajo.

6.4 Sólo los archivos de datos y no los programas ejecutables deberán ser copiados de una computadora a otra.

6.5 Todo diskette debe, normalmente, estar protegido contra escritura para evitar su posible infección al momento de la lectura.

6.6 El sistema debe cargarse desde de un diskette que sea original, o en su defecto desde una copia, especialmente preparada y verificada para que no contenga virus informático.

6.7 Nunca se deben ejecutar programas de origen desconocido.

6.8 No se debe añadir archivos de datos o programas a diskettes que contienen programas originales.

6.9 Efectuar periódicamente la depuración de archivos en los discos duros de la computadora.

6.10 Deberá utilizarse software original.

Del Procedimiento de Detección

6.11 El procedimiento de detección de virus informático debe garantizar que la posible existencia de un virus en un medio magnético u óptico no ingrese directamente al Sistema. Para ello, el programa de detección de virus debe ser instalado en la memoria, a fin de que permanentemente se controle cualquier medio de almacenamiento que sea utilizado con el equipo de computo.

6.12 Se consideran medios de infección por virus a los siguientes:

- **a)** De un diskette infectado proveniente de una fuente exterior al equipo de cómputo.
- **b)** A través de la adquisición o movimiento de máquinas infectadas al centro de cómputo.
- **c)** A través de los diferentes tipos de comunicación entre equipos de cómputo.

6.13 Cuando el sistema operativo está infectado se presentan cualquiera de los síntomas siguientes:

- **a.** El cargado de los programas toma más tiempo de lo normal.
- **b.** Demora excesiva en los accesos al disco, cuando se efectúan operaciones sencillas de escritura .
- **c.** Se producen inusuales mensajes de errores.
- **d.** Encendido de las luces de acceso a dispositivos, cuando no son requeridos en ese momento
- **e.** Disposición de menos memoria de lo normal.
- **f.** Desaparecen programas o archivos misteriosamente.
- **g.** Se reduce repentinamente el espacio del disco.
- **h.** Los archivos ejecutables cambian de tamaño.
- **i.** Aparecen inexplicablemente algunos archivos escondidos.

j. Aparecen en la pantalla una serie de caracteres especiales sin ninguna explicación lógica.

Del Procedimiento de Eliminación de Virus

6.14 Al detectar virus en un equipo de cómputo, se deben seguir los pasos siguientes:

1º Apagar el equipo y todos los dispositivos conectados a él.

2º Colocar un diskette de arranque del computador, protegido contra escritura, que contenga el Sistemas Operativo y archivos de detección y eliminación de virus.

3º Si no cuenta con tal diskette, prepararlo en un equipo que no tenga virus, o solicitarlo al area de Soporte Técnico de la Institución.

4º Encender el sistema y rastrear en las unidades adicionales la presencia de virus, especialmente a los discos duros y/o particiones de los mismos.

5º Detectados los virus, eliminarlos usando el programa antivirus establecido por el órgano competente de la institución.

6º Repetir el paso 4 para mayor seguridad.

7º En el caso de una Red, el Administrador de la red deberá eliminar los virus informáticos.

6.15 Dependiendo de la gravedad del daño ocasionado por el virus, si es necesario, se reconstruirá el sistema. Este proceso lo debe realizar personal de soporte técnico.

VI. Web donde se puede Encontrar Información

- **COMPUTER ASSOCIATES:**
  Sitio web de esta empresa de software que cuenta con una fantástica cobertura informativa sobre el nuevo virus Love Letter. Idioma: Inglés.
  www.ca.com

- **F-SECURITY:**
  Sitio web de esta empresa de seguridad informática dedicada a detectar la aparición de nuevos virus y resolverlos. Contiene un articulo dedicado a el virus Love Letter. Idioma: Inglés.
  www.f-secure.com

- **MCAFFE:**
  Web de este antivirus que permite hacer un analizar el disco duro online parar detectar el nuevo virus Love Letter. Idioma: Inglés.
  www.mcafee.com

- **SINUTEC:**
  Web de la empresa Sinutec Data Security especializada en seguridad y protección de sistemas informáticos. Idioma: Español.
  www.sinutec.com

- **SECURITY FOCUS:**
  Una de las publicaciones líderes en el campo de la seguridad con noticias, vulnerabilidades y agujeros que se actualiza a diario. Idioma: Inglés.
  www.securityfocus.com

- **CERT:**
  Centro de coordinación del CERT, un organismo encargado de avisar y en su caso solucionar los fallos de seguridad causados en la Red, como pueden ser los virus de gusano. Idioma: Inglés.
  www.cert.org

- **NORTON ANTIVIRUS:**
  Sitio web de la empresa Symantec que permite descargarse la última actualización de su antivirus 'Norton' para defenderse del virus Love Letter. Idioma: Inglés.

www.symantec.com

- **PACKET STORM:**
  Sitio web dedicado a la seguridad informática con las últimas noticias sobre virus. Idioma: Inglés.
  http://packetstorm.security.com

- **TREND MICRO:**
  Sitio web de esta empresa de software de seguridad informática que ofrece en sus páginas la solución al virus Love Letter. Idioma: Inglés.
  www.antivirus.com/vinfo

- **SOPHOS ANTI-VIRUS:**
  Últimas noticias y actualizaciones sobre el virus Love Letter para todo aquel que tenga el antivirus Sophos instalado en su computador. Idioma: Inglés.
  www.sophos.com/virusinfo/analyses/vbsloveleta.html

- **KRIPTÓPOLIS:**
  Revista independiente sobre criptografía, seguridad y privacidad en Internet. Idioma: Español
  www.kriptopolis.com/noticias/20000504b.html