

Contenido

Uso de F-Secure Anti-Virus

Descripción general

F-Secure Anti-Virus Gatekeeper

Escaneo manual en busca de virus

Asistente de desinfección

Parámetros del usuario de F-Secure Anti-Virus

Parámetros

Protección en tiempo real

Escaneo manual

Actualizaciones

Estadísticas

Soporte técnico

Soporte técnico

Acerca de F-Secure Corporation

Información empresarial

Familia de productos de F-Secure

Descripción general

F-Secure Anti-Virus se ha diseñado para entornos de redes empresariales. Las características de detección de virus funcionan en tiempo real y con transparencia. Los usuarios apenas tienen que realizar acciones en el programa, lo que disminuye la necesidad de formación y de asistencia. Las características de administración centralizada basada en políticas suponen una solución contra los virus de costes reducidos y fácil mantenimiento.

F-Secure Anti-Virus Gatekeeper

El funcionamiento de F-Secure Anti-Virus Gatekeeper se basa en la tecnología Dynamic Virus Protection. Esta tecnología emplea un controlador de dispositivos que controla los servicios del sistema operativo que se utilizan al abrir archivos y administrar particiones de disco.

La característica de protección en tiempo real que proporciona F-Secure Anti-Virus Gatekeeper supone una protección continua contra virus cuando los archivos se abren, se copian, se mueven, se cambian de nombre o se descargan desde la Web.

La protección en tiempo real funciona de manera transparente en segundo plano, buscando virus siempre que se accede a archivos del disco duro, de disquetes o de unidades de red. Si intenta acceder a un archivo infectado, la protección en tiempo real evitará automáticamente que el virus se ejecute. A continuación, lo eliminará del archivo o emitirá una advertencia, según lo especificado en la política de seguridad.

- F Para evitar que los virus del sector de arranque se propaguen, la protección en tiempo real también comprueba los disquetes al apagar o reiniciar el ordenador. Esta operación puede generar un sonido si no hay ningún disquete en la unidad correspondiente. Este sonido es normal.
-

Para saber si la protección en tiempo real está activa, haga doble clic en el icono de Configuración y estadísticas de F-Secure de la bandeja de sistema situada en la esquina inferior derecha de la pantalla. Si el estado de F-Secure Anti-Virus es 'Activado', la protección en tiempo real está activa, lo que supone una protección continua.

Escaneo manual en busca de virus

No es necesario escanear los archivos manualmente. La característica de detección en tiempo real de F-Secure Anti-Virus Gatekeeper asegura la mejor protección contra virus de forma automática. La información que aparece aquí es de referencia para casos en los que desee llevar a cabo un escaneo manual.

Puede iniciar un escaneo en busca de virus de las siguientes maneras:

- Menú de acceso directo (doble clic en un archivo, carpeta o disco)
- Menú Configuración y estadísticas de F-Secure en la bandeja de sistema (haga clic con el botón derecho en el icono 'F' (F-Secure) de la bandeja de sistema)
- Menú Inicio de Windows (haga clic con el botón derecho en el menú)

Durante el escaneo manual, el cuadro de diálogo *Estadísticas de escaneo manual* muestra un indicador de progreso y las estadísticas del escaneo. Se puede interrumpir el escaneo haciendo clic en **Detener**. Una vez finalizado el escaneo, se genera un informe. Para visualizar el informe en el explorador Web, haga clic en **Mostrar informe**.

Más información:

[Menú de acceso directo](#)

[Menú Configuración y estadísticas de F-Secure en la bandeja del sistema](#)

[Escaneo desde el menú Inicio de Windows](#)

Menú de acceso directo

Para escanear un archivo, carpeta o disco en busca de virus, haga clic con el botón derecho del ratón en el icono y seleccione

‘Escanear carpetas en busca de virus’ en el menú de acceso directo. De esta forma puede escanear cualquier archivo, carpeta o unidad, independientemente de la extensión.

Menú Configuración y estadísticas de F-Secure en la bandeja de sistema.

Puede visualizar el menú Configuración y estadísticas de F-Secure haciendo clic con el botón derecho en el icono 'F' (F-Secure) en la bandeja de sistema.

Para iniciar el escaneo, seleccione una de las acciones de escaneo del menú.

Si selecciona *Escanear objetivo*, tendrá que seleccionar posteriormente la carpeta o disco que va a escanear.

Escaneo desde el menú Inicio de Windows

El grupo de programas de F-Secure Anti-Virus contiene accesos directos para escanear discos duros, disquetes y carpetas.

Para iniciar el escaneo, seleccione uno de los siguientes comandos del menú: *Escanear todos los discos duros locales*, *Escanear disquete* o *Escanear objetivo*. Si selecciona *Escanear carpeta*, tendrá que seleccionar la carpeta o disco que desea escanear.

Asistente de desinfección

Si se detecta un virus mientras está utilizando el ordenador, F-Secure Anti-Virus iniciará de manera predeterminada al asistente de desinfección.

1. La primera pantalla muestra los nombres de los virus que se han detectado.
Para obtener más información acerca de un virus, haga clic en su nombre y, a continuación, en el botón **Información sobre virus**. La página Información sobre virus mostrará una lista de los virus detectados. Puede examinar toda la base de datos de información sobre virus haciendo clic en la casilla de verificación. Si el virus es muy reciente, puede que no aparezca en la base de datos. Si no ve una descripción, puede encontrarla en la base de datos de información sobre virus disponible en nuestro sitio Web.
La base de datos de información sobre virus de F-Secure es una completa base de datos acerca de los virus que además contiene información sobre miles de ellos. Esta base de datos se actualiza todos los días. Para acceder a ella, haga clic en el botón **Club Web**.
2. A continuación, aparecerá una lista con los archivos infectados.
En el cuadro de diálogo **Acción**, seleccione la acción que se va a llevar a cabo sobre los archivos infectados.
3. Los archivos se desinfectarán y aparecerán los resultados de la acción de desinfección.
4. Se generará un informe sobre la desinfección. Si no desea que se genere el informe, desactive la casilla de verificación **Generar informe**.

El informe de desinfección aparece automáticamente. En caso de que el programa tenga administración central, se envía el informe al administrador.

F Nota. El administrador puede configurar F-Secure Anti-Virus para que elimine automáticamente los virus de cualquier ordenador sin solicitar permiso para realizar ninguna acción. En este caso, no se ejecuta el asistente de desinfección.

Parámetros

Los parámetros de F-Secure Anti-Virus se pueden visualizar y modificar. Para ello, abra el cuadro de diálogo *Configuración y Estadísticas de F-Secure* y haga doble clic en el icono 'F' de la bandeja de sistema. Este cuadro de diálogo se abrirá y mostrará una lista de los productos F-Secure instalados.

Puede hacer doble clic en la aplicación *F-Secure Anti-Virus* o hacer clic en **Propiedades** para abrir el cuadro de diálogo *Propiedades de F-Secure Anti-Virus*. En este cuadro puede especificar distintos parámetros para los tres tipos de operaciones de escaneo: Protección en tiempo real, Escaneo manual y Actualizaciones. El cuadro de diálogo *Propiedades de F-Secure Anti-Virus* también tiene información sobre estadísticas de escaneo.

Estadísticas

Muestra los resultados del escaneo en tiempo real.

Protección en tiempo real

Parámetros para la protección continua y transparente que proporciona F-Secure Anti-Virus mientras se ejecuta en segundo plano, escaneando los archivos en el momento en que se accede a ellos.

Escaneo manual

Parámetros para las tareas de escaneo que se inician de manera manual.

Actualizaciones

Parámetros para activar de forma automática los avisos de actualización de la base de datos de definición de virus destinados a las actualizaciones manuales. El botón **Actualizar ahora** permite realizar actualizaciones inmediatas.

Los escaneos en tiempo real deberían estar restringidos para evitar que no utilicen una gran cantidad de recursos del sistema, hecho que puede ocurrir al escanear archivos comprimidos y otros archivos especiales.

Debido a que los escaneos manuales sólo se realizan cuando lo desea el usuario, se pueden definir para que escaneen grandes grupos de archivos, lo que consume más recursos del sistema.

Protección en tiempo real

Para activar o desactivar la protección en tiempo real con F-Secure Anti-Virus, active o desactive la casilla de verificación *Activar protección*.

Más información:

[Acción sobre archivos infectados](#)

[Opciones de escaneo](#)

Acción sobre archivos infectados

En el cuadro de diálogo *Acción sobre archivos infectados*, puede seleccionar la acción que va a realizar F-Secure Anti-Virus al detectar un archivo infectado. Seleccione una de las siguientes acciones:

Preguntar tras escanear

Inicia el asistente de desinfección al detectar un archivo infectado.

Desinfectar automáticamente

Desinfecta el archivo automáticamente al detectar un virus.

Cambiar nombre automáticamente

Cambia el nombre del archivo automáticamente al detectar un virus.

Eliminar automáticamente

Elimina el archivo automáticamente al detectar un virus.

Opciones de escaneo

En *Opciones de escaneo*, puede seleccionar los archivos que se van a escanear en tiempo real.

Puede elegir entre las siguientes opciones:

Todos los archivos

Se escanearán todos los archivos, independientemente de la extensión. No es una opción recomendada, porque podría reducir considerablemente el rendimiento del sistema.

Archivos con estas extensiones

Se escanearán los archivos con las extensiones especificadas. Para especificar archivos sin extensión, escriba ‘.’ Puede utilizar el comodín ‘?’. Introduzca cada extensión de archivo separada por un espacio. Esta opción se recomienda para protección en tiempo real.

Excluir archivos con estas extensiones

Puede especificar los archivos que no se van a escanear.

Excluir objetos

Puede especificar archivos o carpetas individuales que no se van a escanear. Para ello, haga clic en el botón **Seleccionar** y busque los archivos o carpetas que desea que no se escaneen.

Escanear archivos comprimidos

Active esta casilla de verificación para escanear archivos comprimidos, como ZIP, ARJ y LZH. Al escanear grandes archivos comprimidos, puede que se utilice un gran número de recursos del sistema y disminuya la velocidad del sistema. Por tanto, no se recomienda utilizarlo con protección en tiempo real.

Escaneo manual

Puede especificar los parámetros para las operaciones de escaneo manual en la página *Escaneo manual* del cuadro de diálogo *Propiedades de F-Secure Anti-Virus*.

Más información:

[Acción sobre archivos infectados](#)

[Opciones de escaneo](#)

Acción sobre archivos infectados

En el cuadro de diálogo *Acción sobre archivos infectados*, puede seleccionar la acción que va a realizar F-Secure Anti-Virus al detectar un archivo infectado.

Puede seleccionar una de estas opciones:

Preguntar tras escanear

Inicia el asistente de desinfección al detectar un archivo infectado.

Desinfectar automáticamente

Desinfecta el archivo automáticamente al detectar un virus.

Cambiar nombre automáticamente

Cambia el nombre del archivo automáticamente al detectar un virus.

Eliminar automáticamente

Elimina el archivo automáticamente al detectar un virus.

Opciones de escaneo

En *Opciones de escaneo*, puede seleccionar los archivos que desea escanear durante la operación de escaneo manual.

Puede elegir entre las siguientes opciones:

Todos los archivos

Se escanearán todos los archivos, independientemente de la extensión. No se recomienda esta opción porque podría reducir considerablemente el rendimiento del sistema.

Archivos con estas extensiones

Se escanearán los archivos con las extensiones especificadas. Introduzca cada extensión de archivo separada por un espacio. Puede utilizar el comodín '?'.

Excluir archivos con estas extensiones

Puede especificar los archivos que no se van a escanear.

Excluir objetos

Puede especificar archivos o carpetas individuales que no se van a escanear. Para ello, haga clic en el botón **Agregar** y busque los archivos o carpetas que desea que no se escaneen.

Escanear archivos comprimidos

Active esta casilla de verificación para escanear archivos comprimidos, como ZIP, ARJ y LZH. Esta opción se puede utilizar sin problemas, ya que las tareas de escaneo manual no afectan al rendimiento del sistema.

El botón **Escanear ahora** se puede utilizar para escanear una carpeta en busca de virus en cualquier momento.

Actualizaciones

La página Actualizaciones posee información acerca de los motores de escaneo instalados y las actualizaciones de bases de datos de virus. También tiene un enlace directo desde el botón **Más información** al sitio Web de F-Secure o a un sitio ISP.

Más información:

[Motores de escaneo instalados](#)

[Actualizaciones de bases de datos de virus](#)

[Recordar actualizaciones](#)

[Actualizar ahora](#)

[Aviso de actualización](#)

[Más información](#)

Motores de escaneo instalados

En el cuadro de diálogo *Motores de escaneo instalados* puede encontrar información sobre los nombres de motores de escaneo instalados actualmente, las fechas de las bases de datos individuales y sus números de revisión. Los motores de escaneo utilizados son F-Secure F-Prot, F-Secure AVP o F-Secure Orion.

Actualizaciones de bases de datos de virus

La sección *Actualizaciones de bases de datos de virus* facilita información acerca del estado actual de las bases de datos de definición de virus. Por ejemplo, informa de que se deberían realizar actualizaciones inmediatas si las bases de datos de definición están obsoletas.

Recordar actualizaciones

Con la casilla de verificación **Recordar actualizaciones** puede activar los avisos automáticos de actualización de bases de datos de definición de virus. Puede determinar con qué frecuencia debe aparecer un cuadro de diálogo de actualizaciones insertando un número en la casilla **días**.

La disponibilidad de la función del aviso de actualización se determina mediante los parámetros de la política. Si los parámetros de la política han prohibido las actualizaciones manuales, las casillas de verificación **Recordar actualizaciones** y **[X] días** no estarán disponibles. El administrador puede cambiar el estado de permiso de estas opciones de la política de F-Secure Administrator:

FSAV\F-Secure Corporation\F-Secure Anti-Virus\Parámetros\Actualizaciones de bases de datos de virus\Aviso de actualización\Estado de aviso

El estado predeterminado para el modo standalone es **admitido** y para el modo de administración centralizada, **no admitido**.

Actualizar ahora

El botón **Actualizar ahora** inicia las actualizaciones manuales de bases de datos de definiciones de virus. Los parámetros de la política determinan si esta característica está disponible o no.

Si el parámetro de la política de F-Secure Administrator

FSAV\F-Secure Corporation\F-Secure Anti-Virus\Parámetros\Actualizaciones de bases de datos de virus\Permitir actualizaciones manuales

se define como **verdadero**, se puede utilizar el botón **Actualizar ahora**. Si se ha instalado F-Secure Anti-Virus con la configuración de administración centralizada, se iniciará un rastreo de actualización normal desde Management Server o desde el punto en que se distribuyan las bases de datos de definición de virus. El modo standalone inicia la descarga de nuevas bases de datos desde el sitio de F-Secure o desde un sitio ISP.

Aparece un cuadro de diálogo durante el proceso de descarga. Se puede cancelar la actualización haciendo clic en el botón **Cancelar actualización**.

Aviso de actualización

Si se permiten actualizaciones manuales de bases de datos de definición de virus, también estarán activados los avisos de actualización. Si ha activado la casilla de verificación **Recordar actualizaciones cada [X] días** y han pasado X días desde la última actualización o aviso de actualización, aparece un cuadro de diálogo.

Si pulsa el botón **Actualizar ahora** de este cuadro, se inicia la actualización manual de bases de datos de definiciones de virus. Si pulsa el botón **Recordar más tarde**, el aviso de actualización se pospone el número de días seleccionados como intervalo de aviso. Si pulsa el botón **Opciones de actualización**, se abre el cuadro de diálogo *Propiedades de F-Secure Anti-Virus* con la ficha *Actualizaciones* activa.

Más información

El botón **Más información** abre un explorador Web predeterminado en el sitio de F-Secure o de ISP. Se puede cambiar la URL en F-Secure Administrator, en:

FSAV\F-Secure Corporation\F-Secure Anti-Virus\Parámetros\Actualizaciones de bases de datos de virus\Sitio de información

Tenga en cuenta que la URL debe contener el protocolo y el nombre del sitio; por ejemplo <http://www.company.com>

Estadísticas

La página *Estadísticas* del cuadro de diálogo *Propiedades de F-Secure Anti-Virus* muestra los resultados del escaneo en tiempo real para la sesión actual.

Soporte técnico

El soporte técnico de F-Secure está disponible por correo electrónico y a través de nuestro sitio Web. Puede acceder al sitio Web desde F-Secure Anti-Virus o desde el explorador Web.

Más información:

[Club Web](#)

[Descripciones de virus en la Web](#)

[Soporte por correo electrónico](#)

Club Web

El Club Web de F-Secure Anti-Virus proporciona asistencia a los usuarios del producto. Para acceder a ella, seleccione el comando Club Web del menú Ayuda. La primera vez que utilice esta opción, debe introducir la ruta y el nombre del explorador Web y la ubicación.

Para conectar al Club Web directamente desde el explorador Web, vaya a:

<http://www.F-Secure.com/webclub/>

Para obtener soporte avanzado de F-Secure Anti-Virus Support Center, vaya a:

<http://www.F-Secure.com/support/>

Descripciones de virus en la Web

F-Secure Corporation mantiene una completa recopilación de información relacionada con los virus en el sitio Web. Para consultar la base de datos de información sobre virus, seleccione el comando Descripciones de virus en la Web del menú Ayuda.

También puede acceder a la base de datos de información sobre virus en la dirección:

<http://www.F-Secure.com/vir-info/>

Soporte por correo electrónico

Si tiene alguna duda sobre F-Secure Anti-Virus que no haya sido resuelta en el manual o en los servicios en línea de www.F-Secure.com, puede ponerse en contacto con el proveedor local de F-Secure o directamente con F-Secure Corporation.

Para obtener asistencia técnica básica, póngase en contacto con el socio comercial de F-Secure local. Envíe su correo electrónico a:

Anti-Virus-<país en inglés>@F-Secure.com

Ejemplo: Anti-Virus-Norway@F-Secure.com

Si no hay ningún socio comercial autorizado de F-Secure Anti-Virus en su país, puede solicitar asistencia técnica básica en:

Anti-Virus-Support@F-Secure.com

Incluya la siguiente información en la solicitud de soporte:

Número de versión de F-Secure Anti-Virus (incluido el número de revisión).

Nombre y número de versión del sistema operativo (DOS, Windows). Incluya el número de revisión.

Descripción detallada del problema, incluido cualquier mensaje de error del programa y otros detalles que puedan ayudar a reproducir el problema.

Si se pone en contacto con el soporte de F-Secure por teléfono, realice lo siguiente para ahorrar tiempo:

Permanezca frente al ordenador para poder seguir las instrucciones que proporcione el técnico de soporte o prepárese para anotarlas.

Mantenga el ordenador encendido y, si es posible, en el estado en el que se encontraba cuando se produjo el error; también se puede preparar para reproducir el problema en el ordenador sin tener que realizar un gran esfuerzo.

Si se ha producido una infección por virus, asegúrese de que ha ejecutado la última actualización de F-Secure. Puede descargarla del Club Web.

Información empresarial

F-Secure Corporation (anteriormente Data Fellows) es uno de los mejores desarrolladores de productos de protección de datos del mundo. La compañía desarrolla, comercializa y admite productos de software antivirus, de protección de datos y de encriptación redes empresariales. Sus sedes principales se encuentran en San José, California (EE.UU.) y Espoo (Finlandia) y cuenta con sucursales en varios países, incluidos Reino Unido, Francia, Alemania, Japón, Hong Kong y Canadá. Sus socios empresariales, minoristas y distribuidores se encuentran en más de 80 países de todo el mundo. Los productos de F-Secure se han traducido a más de 20 idiomas.

Los productos de software de F-Secure han obtenido numerosos galardones y menciones internacionales. F-Secure ha sido declarada una de las 100 mejores compañías de tecnología del mundo por la revista Red Herring, en su número de septiembre de 1998. La revista de informática SECURE ha premiado a F-Secure Workstation Suite 4.0 con 5 estrellas, la más alta puntuación, en el número de julio de 1999. F-Secure Anti-Virus recibió el galardón por el reconocimiento de los editores de la revista alemana PC Professionell en su número de julio de 1999. También ha obtenido las distinciones de mejor producto del año 1997 (revista Data Communications), mejor producto antivirus (revista SVM, mayo de 1997) y el galardón a la tecnología de información europea de 1996.

F-Secure Corporation posee decenas de miles de clientes en más de 100 países. Entre ellos se encuentran muchas de las principales empresas industriales del mundo y de las compañías de telecomunicaciones más conocidas, así como las principales líneas aéreas internacionales, varios gobiernos europeos, compañías postales, fuerzas militares y algunos de los bancos más importantes del mundo. Entre sus clientes están la NASA, las fuerzas aéreas norteamericanas, la división de sanidad del departamento de defensa y el centro de asuntos bélicos navales de EE.UU, San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera (anteriormente Telecom Finland), UUNet Technologies, Boeing, Bell Atlantic y MCI.

Familia de productos de F-Secure

Todos los productos de F-Secure están integrados en **F-Secure Framework**, que proporciona una administración de tres niveles ampliable, basada en políticas para minimizar el coste de la administración de seguridad.

F-Secure Workstation Suite incorpora funciones de detección y eliminación de códigos maliciosos, cifrado sencillo de archivos y redes y firewall personal, todo integrado en una arquitectura de administración basada en políticas.

F-Secure Anti-Virus; este producto, que incorpora múltiples motores de escaneo (incluidos F-PROT y AVP), es el sistema de protección y escaneo de virus en tiempo real más completo para las principales plataformas de escritorios y de servidores. Es una solución de tres niveles orientada hacia el mercado empresarial e incluye gran cantidad de características para la administración de redes y el despliegue centralizado.

F-Secure Content Scanner protege las redes contra virus que llegan mediante correos electrónicos, descargas de la Web copias de bases de datos. Funciona con Microsoft Exchange Server, Lotus Domino y productos firewall de Check Point y otros importantes proveedores.

F-Secure VPN+ ofrece una solución de red privada virtual, compatible con IPSec y basada en software, para grandes redes empresariales y redes de oficinas remotas y pequeñas. Al combinar los productos de F-Secure VPN+, las empresas de cualquier tamaño pueden utilizar redes públicas de bajo coste o Internet para crear VPN seguros sin necesidad de instalar hardware especial.

F-Secure FileCrypto es el primer y único producto que integra un cifrado de alta seguridad en tiempo real directamente en el sistema de archivos de Windows. Cifra los datos automáticamente antes de almacenarlos en el disco duro, protegiendo la información importante en las situaciones más exigentes. FileCrypto también permite enviar por correo electrónico paquetes cifrados y autoextraíbles a otros usuarios.

FSecure SSH proporciona un login remoto seguro, un terminal y otras conexiones en redes sin seguridad. Es la herramienta de administración remota segura más utilizada.

F-Secure NameSurfer es la solución para administración de DNS de Internet e intranet remotos. Su interfaz de usuario WWW, de fácil utilización, automatiza y simplifica la administración de DNS.

F-Secure Distributed FireWall es un producto firewall basado en software que ofrece protección completa para plantillas muy repartidas y de gran movilidad desde una ubicación con administración central.

Glosario de términos

Control de acceso

AUTOEXEC.BAT

Tarea de fondo

Archivo BAT

BIOS

Bit

Arranque

Sector de arranque

Byte

Suma de comprobación

CMOS

Arranque en frío

Archivo COM

CONFIG.SYS

CounterSign

CPU

CRC

DOS

Archivo EXE

HPFS

Kilobyte

LAN

MBR

Megabyte

Módem

Virus multipartito

Virus mutante

NFS

NTFS

Escáner al acceder

Escáner a petición

RAM

Escáner en tiempo real

Reiniciar

Control de acceso

Procedimiento que otorga o niega la utilización de un sistema a usuarios o procesos. Suele implicar la autenticación del usuario, la verificación de los derechos de acceso, el control y el registro.

AUTOEXEC.BAT

Archivo de comandos que se ejecuta de forma automática durante el inicio del sistema en DOS.

Tarea de fondo

Tarea que se está ejecutando, pero que no aparece en la ventana activa.

Archivo BAT

Archivo que contiene los comandos de DOS que se utilizan para automatizar tareas repetitivas.

BIOS

Sistema de entrada/salida básico (*Basic Input/Output System*). Parte del sistema operativo que gestiona las tareas más relacionadas con el hardware. En la mayoría de los PC, la BIOS se almacena en la memoria ROM.

Bit

Unidad más pequeña de memoria que puede reconocer un ordenador. Un conjunto de bits forma un byte, que se organizan en patrones secuenciales para expresar textos, números u otra información detallada.

Arranque

Reiniciar el ordenador.

Sector de arranque

Registro de arranque. Área situada en la primera pista de disquetes y discos lógicos. La información del sector de arranque permite al ordenador leer un sistema operativo (como MS-DOS).

Byte

Unidad pequeña de memoria, suficiente para almacenar un carácter alfabético o numérico. Un byte está formado por “bits”, unidades binarias agrupadas en conjuntos (por ejemplo, 00101101) que almacenan pequeñas unidades de información.

Suma de comprobación

Número identificativo que se calcula a partir de las características del archivo, de forma que, si el archivo sufre el más mínimo cambio, la identidad cambia.

CMOS

Semiconductor de óxido metálico complementario (*Complementary Metal Oxide Semiconductor*). Memoria alimentada por batería de los ordenadores PC. El tamaño de esta memoria suele ser de 32 a 50 bytes. CMOS contiene información sobre detalles externos, como discos, fecha y periféricos. No se vacía cuando se apaga el ordenador, siempre que la batería no se descargue.

Arranque en frío

Reiniciar el ordenador apagándolo y encendiéndolo.

Archivo COM

Programa ejecutable de DOS con una estructura simple. El tamaño máximo es 64 kilobytes.

CONFIG.SYS

Archivo de configuración que se ejecuta automáticamente durante el inicio del sistema en DOS.

CounterSign

Marco que integra varios motores de escaneo para ofrecer protección en diferentes niveles, para todos los esquemas de cifrado y compresión posibles, aplicando prácticamente el 100% de la protección contra virus en la empresa con una sola interfaz.

CPU

Unidad central de procesamiento (*Central Processing Unit*). Se trata del “cerebro” del ordenador. Suele alojarse en una “caja”, que puede estar separada del monitor.

CRC

Comprobación de redundancia cíclica (*Cyclic Redundancy Check*). Uno de los métodos de suma de comprobación más comunes. CRC utiliza una firma de 32 bits calculada según el contenido del archivo.

DOS

Sistema operativo de disco (*Disk Operating System*). Es el tipo de sistema más básico; originalmente se utilizaba en todos los ordenadores personales.

Archivo EXE

Archivo o archivo de programas ejecutable; es el tipo de archivo que se ejecuta, al contrario que un documento o archivo de datos.

HPFS

Sistema de archivos de alto rendimiento (*High Performance File System*). Sistema de archivos que utiliza OS/2.

Kilobyte

1.024 bytes

LAN

Red de área local (*Local Area Network*). Red pequeña de una habitación, edificio o grupo, que puede estar o no conectada a Internet.

MBR

Registro de arranque (*Master Boot Record*). Área situada en la pista cero del disco duro físico. Contiene el programa de arranque principal y la tabla de particiones. Es independiente de los sistemas operativos y siempre se ejecuta en primer lugar una vez que el ordenador ha realizado la prueba automática de encendido (POST, *PowerOnSelfTest*). El tamaño de este registro es de 512 bytes. El programa de arranque principal traduce la tabla de particiones, que contiene información sobre la división (partición) del disco físico en entidades lógicas. A continuación, el programa de arranque principal ejecuta el sector de arranque de la partición activa.

Megabyte

1024 kilobytes (un millón de bytes)

Módem

Elemento telefónico de hardware que se utiliza para conectar un ordenador o red de área local a una red más grande, como Internet.

Virus multipartito

Virus compuesto de varias partes. Hay que limpiar cada una de las partes del virus multipartito, para asegurar que no existe riesgo de infección.

Virus mutante

Virus que cambia por sí mismo (muta) según atraviesa los archivos del host, lo que complica la desinfección.

NFS

Sistema de archivos de red (*Network File System*) utilizado por muchas variantes de UNIX.

NTFS

Sistema de archivos de Windows NT (*Windows NT File System*).

Escáner al acceder

Escáner en tiempo real; proceso de fondo que proporciona vigilancia constante contra los virus.

Escáner a petición

Escáner de virus que se inicia de forma manual.

RAM

Memoria de acceso aleatorio (*Random Access Memory*). Memoria dinámica utilizada por el procesador.

Escáner en tiempo real

Escáner que funciona en segundo plano, lo que permite al usuario seguir trabajando a una velocidad normal, sin que ésta disminuya de forma significativa.

Reiniciar

Arrancar el sistema en caliente.

