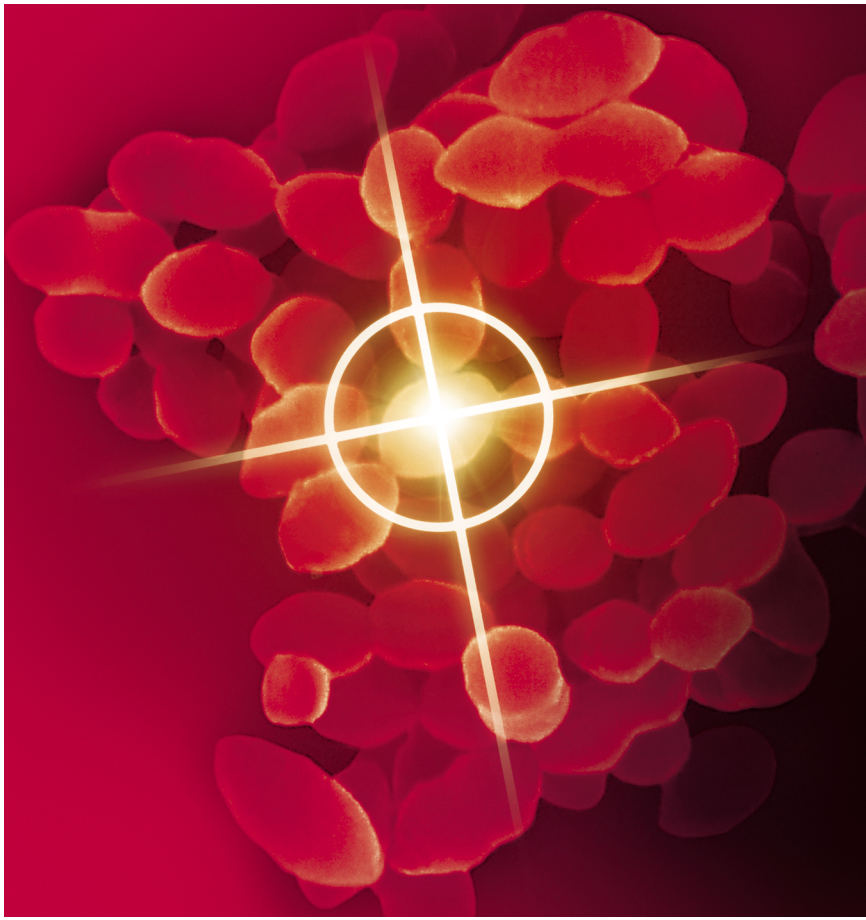
INICIO RÁPIDO

McAfee VirusScan

VERSIÓN 6.0



McAFEE
A Network Associates Business

Contrato de Licencia Perpetua para el Usuario Final de McAfee

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL SIGUIENTE CONTRATO DE LICENCIA (EN ADELANTE, EL "CONTRATO") DEL SOFTWARE ESPECIFICADO (EN ADELANTE, EL "SOFTWARE") POR NETWORK ASSOCIATES INTERNATIONAL B.V. (EN ADELANTE, "MCAFEE"). AL PULSAR EL BOTÓN ACEPTAR O AL INSTALAR EL SOFTWARE, EL USUARIO (PERSONA FÍSICA O ENTIDAD) ACEPTA SU VINCULACIÓN A ESTE CONTRATO Y SE CONVIERTE EN PARTE DEL MISMO. SI EL USUARIO NO ESTÁ DE ACUERDO CON TODAS LAS CONDICIONES DE ESTE CONTRATO, DEBERÁ PULSAR EL BOTÓN QUE INDICA QUE NO SE ACEPTAN LAS CONDICIONES Y SE ABSTENDRÁ DE INSTALAR EL SOFTWARE. (SI PROCEDE, PUEDE DEVOLVER EL PRODUCTO AL LUGAR DONDE LO ADQUIRIÓ Y OBTENER EL REEMBOLSO DEL IMPORTE PAGADO POR EL MISMO.)

1. **Concesión de licencia.** Sujeto al pago de la tarifa correspondiente a la licencia y a las condiciones y términos especificados en este Contrato, McAfee otorga mediante el presente Contrato al Usuario el derecho no exclusivo e intransferible a utilizar una copia de la versión especificada del Software y la documentación adjunta ("Documentación"). El Usuario podrá instalar una copia del Software en un ordenador, una estación de trabajo, un asistente digital personal, un avisador o busca, un "teléfono inteligente" o en otro dispositivo electrónico para el que el Software esté diseñado (individualmente considerados en adelante, "Dispositivo del Usuario"). En caso de otorgar la licencia del Software dentro de un conjunto o paquete de productos de Software especificados, esta licencia se aplicará a todos los productos de Software especificados, sujetos a las restricciones o condiciones de uso determinadas en la lista de tarifas de Software correspondiente o en el embalaje del producto que se apliquen a cualquiera de dichos productos de Software por separado.

    a. **Uso.** La licencia del Software se otorga exclusivamente para un único producto y, por lo tanto, no se podrá utilizar en más de un Dispositivo del Usuario o por más de un Usuario a la vez, salvo lo dispuesto en esta Cláusula 1. Se entiende que el Software está "en uso" en un Dispositivo del Usuario cuando se carga en la memoria temporal (es decir, la memoria de acceso aleatorio o RAM) o cuando se instala en la memoria permanente (es decir, disco duro, CD-ROM u otro dispositivo de almacenamiento) del Dispositivo del Usuario. Esta licencia autoriza a realizar una copia del Software, con la única finalidad de archivar o efectuar copias de seguridad, siempre que dicha copia contenga todos los avisos de propiedad del Software.

b. **Modo Servidor.** El Usuario puede utilizar el Software en un Dispositivo del Usuario o como servidor ("Servidor") en un entorno de varios usuarios o de red ("Modo servidor") solamente en el supuesto de que se autorice este uso del Software en la lista de tarifas correspondiente o en el embalaje del Software. Se necesitará otra licencia para cada Dispositivo del Usuario o "equipo" que se conecte al Servidor en cualquier momento, independientemente de si tales Dispositivos del Usuario o equipos con licencia están conectados de forma simultánea al Software, o bien, acceden o utilizan el mismo. El uso de software o hardware que reduzca el número de Dispositivos del Usuario o equipos que directamente accedan al Software o utilicen el mismo (por ejemplo, software o hardware "multiplexor" o "de agrupamiento"), no reducirá el número de licencias necesarias (es decir, el número de licencias necesarias debe ser igual al número de diferentes entradas al software multiplexor o de agrupamiento o al "programa final" del hardware). Si el número de Dispositivos del Usuario o equipos que se pueden conectar al Software supera el número de licencias concedidas, se deberá disponer de un mecanismo razonable para asegurar que el uso del Software no incumple los límites de uso especificados en la licencia otorgada. Esta licencia autoriza al Usuario a realizar o descargar una copia de la Documentación de cada Dispositivo del Usuario o equipo con licencia, siempre que dichas copias contengan todos los avisos de propiedad de la Documentación.

c. **Licencias por Volumen.** Si la licencia del Software se otorga en base a condiciones de volumen, especificadas en la lista de tarifas correspondiente o en el embalaje del Software, el Usuario podrá realizar, utilizar e instalar la cantidad de copias del Software en el número de Dispositivos del Usuario autorizados en la licencia por volumen. El Usuario deberá disponer de un mecanismo razonable para asegurar que el número de Dispositivos del Usuario en que se ha instalado el Software no supera la cantidad de licencias otorgadas. Esta licencia autoriza al Usuario a realizar o descargar una copia de la Documentación por cada copia adicional autorizada en la licencia de volumen, siempre que dichas copias contengan todos los avisos de propiedad de la Documentación.

2. **Período de vigencia.** Este Contrato tendrá una duración indefinida, a menos que el mismo sea resuelto previamente de conformidad con alguna de sus Cláusulas. El presente Contrato se resolverá de forma automática en el supuesto de que el Usuario incumpla alguna limitación o requisito descrito en el mismo. En el momento de la resolución o expiración del Contrato, el Usuario deberá destruir todas las copias del Software y de la Documentación.

3. **Actualizaciones.** Durante el período especificado en la lista de tarifas de Software correspondiente o en el embalaje del Sofware, el Usuario estará autorizado a descargar revisiones o actualizaciones del Software en el momento y en la forma en que McAfee las publique a través de su sistema de publicación electrónica, sitio web u otros servicios en línea. Durante un período de noventa (90) días a partir de la fecha de la compra licencia original del Software, el Usuario está autorizado a descargar una (1) revisión o actualización del Software en el momento y en la forma en que McAfee las publique a través de su sistema de publicación electrónica, sitio web u otros servicios en línea. Después del período antes especificado, el Usuario no gozará de derecho alguno a recibir ninguna revisión o actualización sin la compra adquisición de una nueva licencia del Software.

4. **Derechos de propiedad.** Este Software se halla protegido por las leyes de derechos de autor de los Estados Unidos y por tratados internacionales. McAfee y sus proveedores son propietarios y mantienen todos los derechos y la titularidad sobre el Software, así como el interés hacia el mismo, incluyéndose todos los derechos de autor, patentes, derechos comerciales secretos, marcas comerciales y demás derechos de propiedad intelectual e industrial aplicables. La

posesión, instalación o utilización del Software por parte del Usuario no transfiere a éste titularidad alguna acerca de la propiedad intelectual del mismo, ni otorga derechos sobre del Software, excepto por lo establecido en los términos establecidos expresamente en este Contrato. Todas las copias del Software y la Documentación realizadas por el presente documento Contrato deberán contener los mismos avisos de propiedad que aparecen en el Software y la Documentación.

5. **Restricciones.** El Usuario no podrá vender, alquilar, licenciar, arrendar o transferir de cualquier forma, gratuita o no, el Software. El Usuario no revelará a terceros los resultados de cualquier test de referencia (benchmark test) realizado sobre el Software sin el previo consentimiento de McAfee por escrito. El Usuario no deberá permitir que terceros (salvo aquellos que hayan suscrito un contrato con el Usuario que contenga obligaciones de confidencialidad no menos restrictivas que las establecidas en el presente Contrato) usen el Programa Licenciado de forma alguna y llevará a cabo todo lo que esté en su mano para impedir que se lleve a cabo un uso impropio o desautorizado del Programa Licenciado. El Usuario no deberá permitir que terceros se aprovechen del uso o funcionamiento del Software en un contrato de oficina de tiempo mediante su uso compartido, contrato de servicios o de otro tipo, excepto en los casos en que dicho uso se especifique en la lista de tarifas correspondiente o en el embalaje del Software. Asimismo, el Usuario no puede transferir los derechos otorgados en este Contrato, ni puede realizar ingeniería inversa, descompilar o desmontar el Software, excepto en la medida en que la ley aplicable prohiba esta restricción de forma expresa. El Usuario no puede: modificar ni crear ningún trabajo derivado de todo el Software o de parte de éste; copiar el Software o la Documentación, excepto de la forma permitida expresamente en la Cláusula 1 anterior; ni eliminar ningún aviso de propiedad o etiquetas del Software. Todos los derechos que no hayan sido mencionados aquí de forma expresa, quedan reservados a McAfee. McAfee se reserva el derecho a realizar inspecciones periódicas, mediando previo aviso por escrito, para comprobar el cumplimiento de las condiciones de este Contrato.

6. **Garantía y renuncia.**

   a. **Garantía limitada.** McAfee garantiza que, durante los sesenta (60) días posteriores al otorgamiento de la licencia, los medios o soportes (por ejemplo, disquetes) que contienen el Software no presentarán defectos de material ni de fabricación.

   b. **Acciones del Usuario.** La única responsabilidad de McAfee y de sus proveedores y la compensación exclusiva que corresponderá al Usuario por cualquier incumplimiento de la garantía anterior será, según criterio de McAfee, (i) la devolución de la cantidad abonada por la licencia, de haber sido ésta abonada, o (ii) la sustitución del medio o soporte defectuoso que contiene el Software. El Usuario deberá devolver el medio o soporte defectuoso a McAfee con una copia de la factura y pagar los gastos de envío. Esta garantía limitada no será válida si el defecto es consecuencia de un accidente o uso incorrecto o abusivo. Cualquier medio o soporte de sustitución reemplazado estará garantizado durante el resto del período de garantía original. Fuera de los Estados Unidos, esta compensación puede no resultar aplicable en la medida en que McAfee esté sujeto a las restricciones establecidas por las leyes y normativas de los Estados Unidos sobre control a la exportación.

c. **Limitaciones a la Garantía.** Salvo por la garantía anteriormente expuesta, EL SOFTWARE SE ENTREGA "TAL Y COMO ESTÁ". EN LA MEDIDA EN QUE LAS LEYES APLICABLES LO PERMITAN, MCAFEE RENUNCIA A OTORGAR CUALESQUIERA GARANTÍAS, TANTO EXPRESAS COMO IMPLÍCITAS, INCLUIDAS, SIN CARÁCTER EXHAUSTIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, ADECUACIÓN A UN DETERMINADO FIN Y NO INFRACCIÓN, RESPECTO AL SOFTWARE Y LA DOCUMENTACIÓN ADJUNTA. EL USUARIO ASUME TODA LA RESPONSABILIDAD EN LA SELECCIÓN DEL SOFTWARE PARA OBTENER LOS RESULTADOS ESPERADOS Y EN LA INSTALACIÓN, USO Y RESULTADOS OBTENIDOS CON EL SOFTWARE. SIN PERJUICIO DE LO ANTERIOR, MCAFEE NO GARANTIZA QUE EL SOFTWARE ESTÉ EXENTO DE ERRORES, INTERRUPCIONES U OTRO TIPO DE FALLOS, NI QUE SE AJUSTE A LAS NECESIDADES DEL USUARIO. ALGUNOS ESTADOS Y JURISDICCIONES NO PERMITEN LAS LIMITACIONES EN LAS GARANTÍAS IMPLÍCITAS, POR LO QUE PUEDE QUE LA LIMITACIÓN ANTERIOR NO SE APLIQUE AL USUARIO ACTUAL. Las disposiciones anteriores serán válidas y exigibles en la medida en que las leyes aplicables lo permitan.

7. **Limitación de responsabilidades.** EN NINGÚN CASO NI DE CONFORMIDAD CON NINGUNA DOCTRINA LEGAL, YA SEA EN MATERIA EXTRACONTRACTUAL, CONTRACTUAL O DE OTRO TIPO, MCAFEE NI SUS PROVEEDORES SERÁN RESPONSABLES ANTE EL USUARIO, O ANTE OTRAS PERSONAS, DE DAÑOS EMERGENTES, ESPECIALES, INCIDENTALES O DERIVADOS NI DE CUALQUIER OTRO TIPO, INCLUIDOS, AUNQUE SIN LIMITARSE A ELLOS, LOS PERJUICIOS DERIVADOS DE LA PÉRDIDA DEL FONDO DE COMERCIO, INTERRUPCIÓN DEL TRABAJO, AVERÍA, FALLO O FUNCIONAMIENTO INCORRECTO DEL ORDENADOR, O TODOS Y CUALESQUIERA TIPOS DE DAÑOS O PÉRDIDAS. EN NINGÚN CASO MCAFEE SERÁ RESPONSABLE DE DAÑOS SUPERIORES A LA TARIFA ESTIPULADA PARA LA LICENCIA DEL SOFTWARE, AUN CUANDO SE HAYA INFORMADO A MCAFEE DE LA POSIBILIDAD DE TALES DAÑOS. ESTA LIMITACIÓN DE RESPONSABILIDAD NO AFECTA A LA RESPONSABILIDAD POR MUERTE O LESIONES PERSONALES EN LA MEDIDA EN QUE LAS LEYES APLICABLES PROHIBAN TAL LIMITACIÓN. POR OTRO LADO, ALGUNOS ESTADOS Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LIMITACIÓN DE DAÑOS INCIDENTALES O DERIVADOS, DE MANERA QUE ES POSIBLE QUE ESTA LIMITACIÓN Y EXCLUSIÓN NO SE APLIQUEN. Las disposiciones anteriores serán válidas y exigibles en la medida en que las leyes aplicables lo permitan.

8. **Gobierno de los Estados Unidos.** El Software y la Documentación adjunta se consideran "software comercial para ordenadores" y "documentación de software comercial para ordenadores", respectivamente, conforme a DFAR Apartado 227.7202 y FAR Apartado 12.212, según proceda. Cualquier uso, modificación, reproducción, publicación, ejecución, revelación o difusión del Software y de la Documentación adjunta por parte del gobierno de los Estados Unidos se regirá exclusivamente según las condiciones del presente Contrato, y estará estando prohibido cualquier uso, modificación, reproducción, publicación, ejecución, revelación o difusión del Software y de la Documentación adjunta, excepto en la medida en que los términos de dicho Contrato lo permitan.

9. **Restricciones a la exportación.** El Usuario declara haber sido advertido de que los Productos están sometidos a las normas administrativas de control a la exportación de los Estados Unidos. El Usuario no deberá exportar, importar o transferir Productos, de forma directa o indirecta, si ello resultare contrario a las leyes de los Estados Unidos u otras legislaciones aplicables, ni aprobará, facilitará o mediará en forma alguna para que otras personas (como agentes o terceros) lo hagan. El Usuario manifiesta y acuerda que ni el Departamento de Administración de las Exportaciones de los Estados Unidos (United States Bureau of Export Administration) ni cualquier otra autoridad administrativa federal norteamericana ha suspendido, revocado o denegado sus derechos de exportación. El Usuario acuerda no emplear ni transferir los Productos para usos finales relacionados con armas nucleares, químicas o biológicas, con tecnología relativa a misiles salvo autorización legal o específica del Gobierno de los Estados Unidos o licencia otorgada al efecto. Adicionalmente, el Usuario reconoce que los Productos están sometidos a las normas de control a la exportación de la Unión Europea y declara y se compromete a que los Productos no sean empleados más que para fines civiles (es decir, no militares). Aunque ambas partes acuerdan colaborar conjuntamente para la obtención de cualquier licencia o autorización necesaria, el Usuario asume la exclusiva responsabilidad a la hora de cumplir con todas y cada una de las leyes de exportación e importación, no existiendo responsabilidad alguna de McAfee tras la venta al Usuario en el país donde aquella fue perfeccionada.

10. **Actividades de alto riesgo.** El Software no está exento de errores y no se ha diseñado ni pensado para ser utilizado en entornos peligrosos que requieran un funcionamiento con protección ante errores, incluyendo, pero no limitándose a, operaciones en instalaciones nucleares, sistemas de comunicación o navegación aérea, control del tráfico aéreo, sistemas de armamento o equipos de protección vital, en los cuales el fallo del cualquier Software podría ser causa directa de muerte, lesiones o daños físicos o daños a la propiedad graves (En adelante conjuntamente denominadas, "Actividades de alto riesgo"). McAfee rechaza expresamente cualquier garantía explícita o implícita de adecuación para Actividades de alto riesgo.

11. **Varios.** Este Contrato se rige por las leyes de España. Se excluye expresamente la aplicación de la Convención de contratos de las Naciones Unidas para la Venta internacional de mercancías. Este Contrato establece todos los derechos del Usuario del Software y representa el contrato íntegro entre las partes. McAfee se reserva el derecho a inspeccionar periódicamente al Usuario para asegurarse de que no se está infringiendo lo dispuesto en este Contrato al usar el Software. Durante el horario de trabajo habitual y previa notificación por escrito al respecto, McAfee podrá realizar una visita a las instalaciones del Usuario y éste deberá facilitar a McAfee o a sus representantes todos los registros relativos al Software. El coste de cualquier inspección será a cargo de McAfee, a menos que la citada inspección revele la existencia de una deuda a favor de McAfee superior al 5% de la tarifa de la licencia de Software inicial o un uso inapropiado del Software, en cuyo caso la inspección será a cargo del Usuario. El presente Contrato sustituye a cualesquiera otras comunicaciones referentes al Software y a la Documentación. Este Contrato podrá ser modificado únicamente mediante anexos por escrito realizados por un representante debidamente autorizado de McAfee. No se aceptará la renuncia

a ninguna de las disposiciones del presente Contrato, a menos que dicha renuncia se presente por escrito y sea firmada por McAfee o por un representante debidamente autorizado de McAfee. Si cualquiera de las disposiciones de este Contrato fuese anulada, el resto del Contrato permanecerá en vigor y mantendrá todos sus efectos. Las partes confirman su deseo de que este Contrato se redacte sólo en español.

12. **CONTACTO DEL USUARIO CON MCAFEE.** Si tiene alguna duda referente a estos términos y condiciones del presente Contrato o desea ponerse en contacto con McAfee por cualquier otra razón, llame al teléfono +31 20 586 61 00, o escriba a la siguiente dirección: Network Associates, S. A. (Unipersonal), Calle Orense 4, 4ª Planta, Edificio Trieste, 28020 Madrid, España. http://www.mcafee-at-home.com.

Tabla de contenido

Bienvenido a McAfee VirusScan 1

¿Cómo funciona el software VirusScan?

El software VirusScan combina el software de exploración más eficaz del sector con excelentes mejoras que proporcionan acceso completo a las capacidades del software. La interfaz gráfica de usuario de VirusScan unifica los componentes de programa especializados sin sacrificar la flexibilidad que el usuario necesita para adaptar el software a su entorno informático. El software de exploración combina las mejores características de las tecnologías desarrolladas independientemente por los investigadores de McAfee y McAfee VirusScan durante más de una década.

¿Qué incluye el software VirusScan?

El software VirusScan incluye varios componentes que combinan uno o más programas relacionados, cada uno de los cuales desempeña una función determinada en la defensa del equipo contra los virus y otro software perjudicial. Estos componentes son:

- **Ventana principal de VirusScan.** Es el punto de entrada central para utilizar todos los componentes disponibles en McAfee VirusScan. La ventana principal ofrece información relevante, como la última vez que se realizó una exploración de virus en el equipo y las opciones actuales de VShield en el equipo. La ventana principal también informa acerca de la disponibilidad de actualizaciones del producto.

  Mediante esta interfaz de fácil utilización, puede obtener acceso a las funciones principales de McAfee VirusScan: simplemente seleccione “Elegir una tarea” para obtener acceso y utilizar todas las características y todos los componentes de VirusScan.

  Para obtener respuestas a preguntas acerca de virus, soporte al producto o ver la ayuda en línea, consulte la sección Consulte también de la ventana principal de VirusScan.

- **Exploración a petición (ODS).** La exploración a petición permite explorar en cualquier momento. Por ejemplo, si sospecha que ha entrado en contacto con un archivo infectado, pero no ha tenido acceso al archivo, puede explorar manualmente el archivo, la carpeta, la unidad, etc. sospechosos.

- **Explorador de VShield.** Es un componente de la **Exploración automática** (**OAS**) que ofrece protección antivirus continua contra los virus que llegan mediante disquetes, desde la red o desde varias fuentes en Internet. El explorador de VShield se inicia cuando arranca el equipo y permanece en memoria hasta que lo apaga. Un conjunto flexible de páginas de propiedades permiten al usuario indicar al explorador las partes del sistema que debe examinar, las que debe omitir y cómo responder ante cualquier archivo infectado que encuentre. Asimismo, el explorador puede advertirle cada vez que encuentre un virus y resumir cada una de sus acciones.

  El explorador de VShield incluye módulos especializados que protegen el sistema contra subprogramas Java y controles ActiveX hostiles, exploran los mensajes de correo electrónico y los datos adjuntos que se reciben desde Internet a través de Microsoft Mail u otros clientes de correo que cumplan con el estándar Interfaz de programación de aplicaciones de mensajería (MAPI) de Microsoft y bloquean el acceso a sitios peligrosos de Internet. La protección de la configuración mediante contraseña evita que otros usuarios realicen cambios no autorizados. El mismo cuadro de diálogo práctico controla las opciones de configuración de todos los módulos de VShield.

- **Hostile Activity Watch Kernel (HAWK).** HAWK supervisa el equipo para buscar actividad sospechosa que pueda indicar que el sistema tiene un virus. Al contrario que VirusScan, que limpia el virus, HAWK evita que los virus, gusanos y caballos de Troya se propaguen.

- **Safe & Sound.** Este componente permite crear conjuntos de copias de seguridad en archivos de volumen protegido, que es el tipo de copia de seguridad más seguro y conveniente. Un *archivo de volumen protegido* es un área independiente de la unidad, en ocasiones denominada unidad lógica.

- **Cuarentena.** Este componente permite mover archivos infectados a una carpeta de cuarentena. Con ello, los archivos infectados se retiran de las áreas donde están accesibles y el usuario puede limpiarlos o borrarlos cuando le resulte conveniente.

- **Utilidad SendVirus.** Esta característica proporciona al usuario un modo sencillo y sin problemas de enviar archivos que pueden estar infectados directamente a los investigadores antivirus de McAfee. Un asistente sencillo le guiará mientras elige los archivos que desea enviar, incluye los detalles de contacto y, si lo desea, elimina cualquier dato personal o confidencial de archivos de documentos.

- **Extensión Exploración del correo electrónico.** Este componente permite explorar el buzón de correo de Microsoft Exchange o Outlook o carpetas públicas a las que tiene acceso, directamente en el servidor. Esta valiosa visión de “rayos x” en su buzón de correo significa que el software VirusScan puede encontrar posibles infecciones antes de que lleguen al equipo de escritorio, lo que puede detener un virus como Melissa.

- **Utilidad para la creación de discos de emergencia.** Esta utilidad esencial le ayuda a crear un disquete que puede utilizar para arrancar su equipo en un entorno libre de virus y, a continuación, explorar las áreas fundamentales del sistema para eliminar los virus que se podrían cargar al iniciarlo.

- **CD de ejecución automática.** El CD de instalación de VirusScan incluye una versión en CD del disco de inicio de emergencia. Si el equipo está configurado para iniciarse en la unidad de CD, puede utilizar el CD para arrancar el equipo en un entorno libre de virus y explorar en busca de los virus que se cargan al iniciarlo.

- **Actualización instantánea.** Permite que el equipo se comunique automáticamente con McAfee mientras está conectado a Internet y consulta la disponibilidad de actualizaciones del producto, actualizaciones de archivos de firma antivirus y actualizaciones del software de exploración de VirusScan. Esta característica también se utiliza para registrar el producto de McAfee.

- **Protección de dispositivos inalámbricos.** Además de la protección antivirus total para su PC, VirusScan protege su dispositivo inalámbrico y su PC de virus dañinos que se transfieren durante el proceso de sincronización.

- **Exploradores de la línea de comandos.** Este componente consiste de un conjunto de exploradores completos que pueden utilizarse para realizar operaciones de exploración dirigidas desde las ventanas MS-DOS o Símbolo del sistema o desde un modo MS-DOS protegido. El conjunto incluye:

  – SCAN.EXE, un explorador únicamente para entornos de 32 bits. Es la interfaz de línea de comandos principal. Al ejecutar este archivo, éste comprueba su entorno para determinar si se puede ejecutar de modo independiente. Si el equipo se ejecuta en modo de 16 bits o en modo protegido, transferirá el control a uno de los demás exploradores.

- SCANPM.EXE, un explorador para entornos de 16 y de 32 bits. Este explorador ofrece un conjunto completo de opciones de exploración para entornos DOS en modo protegido de 16 ó 32 bits. También incluye compatibilidad con asignaciones de memoria extendida y memoria flexible. SCAN.EXE transferirá el control a este explorador cuando sus funciones especializadas puedan permitir que la operación de exploración se ejecute con mayor eficacia.
- SCAN86.EXE, un explorador únicamente para entornos de 16 bits. Este explorador incluye un conjunto limitado de funciones diseñadas para entornos de 16 bits. SCAN.EXE transferirá el control a este explorador si el equipo se ejecuta en modo de 16 bits, pero sin configuraciones de memoria especiales.
- BOOTSCAN.EXE, un explorador especializado más pequeño, utilizado principalmente con la utilidad de disco de emergencia. Este explorador se ejecuta normalmente desde un disquete creado para proporcionar un entorno de arranque libre de virus.

Todos los exploradores de la línea de comandos permiten iniciar operaciones de exploración dirigidas desde una ventana MS-DOS o Símbolo del sistema o desde un modo MS-DOS protegido. Normalmente utilizará la interfaz gráfica de usuario (GUI) de la aplicación VirusScan para la mayoría de las tareas de exploración; no obstante, si tiene problemas para iniciar Windows o no puede ejecutar los componentes GUI de VirusScan desde su entorno, puede utilizar los exploradores de la línea de comandos como copias de seguridad.

Instalación del software VirusScan 2

Antes de comenzar

McAfee distribuye el software VirusScan de dos maneras:

1. Como un archivo que puede descargar desde el sitio Web de McAfee.
2. En CD-ROM.

Aunque el método que se utiliza para transferir archivos de VirusScan desde un archivo obtenido mediante descarga es diferente del método utilizado para transferir archivos desde un CD ubicado en su unidad de CD-ROM, los pasos de instalación que deben seguirse tras la transferencia son los mismos para ambos tipos de distribución. Compruebe los requisitos del sistema que figuran a continuación para asegurarse de que el software VirusScan puede ejecutarse en su sistema.

Requisitos del sistema

Para instalar este producto, se requiere lo siguiente:

Equipos de escritorio y portátiles

- Windows 95B, Windows 98, Windows Me, Windows NT Workstation con Service Pack 4 o posterior, Windows 2000 Professional, Windows XP Home Edition o Windows XP Professional.
- 35 megabytes (MB) de espacio en disco duro.
- 32 MB de RAM.
- Un procesador Intel de tipo Pentium o compatible a 100 MHz o superior.
- Unidad de CD-ROM.
- Acceso a Internet para actualizar el producto.

Requisitos adicionales para dispositivos inalámbricos

Requisitos para Palm OS ® y Palm ™

McAfee VirusScan para Palm ™ Desktop con HotSync ® Manager 3.0 se puede instalar y ejecutar en cualquier PC IBM o compatible con Palm ™ Desktop 3.0 o posterior. La última versión de Palm ™ Desktop y HotSync ® 3.0 puede descargarse gratis desde el sitio Web de Palm (en www.palm.com). La porción residente del dispositivo es bastante sencilla y debería funcionar en cualquier dispositivo equipado con Palm OS ®.

Requisitos del sistema para Windows ® CE ® o Pocket PC

McAfee VirusScan para Windows ® CE ® o Pocket PC se puede instalar y ejecutar en cualquier PC IBM o compatible con ActiveSync 3.0 o posterior. Cualquier dispositivo CE con ActiveSync 3 funcionará correctamente.

Requisitos del sistema para EPOC de Symbian

McAfee VirusScan para EPOC de Symbian se puede instalar y ejecutar en cualquier PC IBM o compatible equipado con PsiWin 2.3 (o equivalente para dispositivos EPOC sin Psion). Todos los dispositivos EPOC deberían contar con PsiWin 2.3 / EPOC Connect 5. Entre éstos se incluyen:

- Psion Revo
- Psion Series 5mx
- Psion Series 7
- Psion netBook
- Oregon Scientific Osaris
- Ericsson MC218
- Ericsson R380

Si tiene un dispositivo más antiguo con el software PsiWin / EPOC Connect actual, McAfee VirusScan para EPOC de Symbian funcionará correctamente, incluyendo Psion HC, la serie MC, la serie Workabout, todos los modelos Psion Series 3, Psion Siena, Psion Series 5, Geofox One y Phillips Illium.

Si no posee PsiWin 2.3, Symbian le ofrece un producto gratuito denominado EPOC Connect Lite, que también funciona.

Otras recomendaciones

Para obtener el máximo provecho de las características de actualización instantánea automática del software VirusScan debe disponer de conexión a Internet, bien sea a través de la red de área local o a través de un módem de alta velocidad y un proveedor de servicios Internet.

Opciones de instalación

La sección “Procedimiento de instalación” describe cómo instalar el software VirusScan con las opciones más comunes en un sólo equipo o estación de trabajo. Puede realizar una instalación Característica, que instala los componentes de VirusScan habitualmente utilizados, o bien una instalación Personalizada, que le ofrece la opción de instalar todos los componentes de VirusScan.

Procedimiento de instalación

IMPORTANTE: Como el programa de instalación instala algunos archivos de VirusScan como servicios en sistemas Windows NT Workstation v4.0, Windows 2000 Professional y Windows XP, debe iniciar una sesión en su equipo con un perfil de usuario que tenga derechos administrativos para instalar este producto. Para ejecutar el programa de instalación en Windows 95, Windows 98 y Windows Me no necesita iniciar la sesión con un perfil o derecho en particular.

McAfee recomienda salir de todas las aplicaciones que se estén ejecutando en el sistema antes de iniciar la instalación. De este modo, se reduce la posibilidad de que conflictos de software interfieran con la instalación.

Tras insertar el CD de instalación de McAfee VirusScan en la unidad de CD-ROM, deberá aparecer automáticamente la imagen de ejecución automática de VirusScan. Para instalar el software VirusScan inmediatamente, haga clic en **Instalar VirusScan** y, a continuación, vaya al paso 5 en la página 18 para continuar con la instalación.

Siga los pasos que figuran a continuación para instalar el software VirusScan.

1. Si su equipo ejecuta Windows NT Workstation v4.0, Windows 2000 Professional o Windows XP, inicie la sesión en el sistema con un usuario con derechos administrativos. Debe poseer derechos administrativos para instalar el software VirusScan en su sistema.

2. Introduzca el CD de VirusScan en la unidad de CD-ROM de su equipo. Si el Asistente para la instalación de VirusScan no aparece automáticamente, vaya al paso 3. En caso contrario, omita este paso y vaya al paso 4.

3. Utilice el procedimiento siguiente si el menú de instalación de ejecución automática no aparece, o si obtuvo el software mediante descarga en un sitio Web de McAfee.

   a. En el menú Inicio de Windows, seleccione **Ejecutar**. Aparecerá el cuadro de diálogo Ejecutar.

   b. Escriba `<X>:\SETUP.EXE` en el cuadro de texto y haga clic en **Aceptar**.

      La `<X>` representa la letra de la unidad de CD-ROM o la ruta de acceso a la carpeta que contiene los archivos VirusScan extraídos. Para buscar los archivos correctos en el disco duro o en el CD-ROM, haga clic en **Examinar**.

4. Antes de continuar con la instalación, el programa de instalación comprueba si su equipo ya ejecuta la herramienta Microsoft Windows Installer (MSI) como parte del software del sistema.

   a. Si el equipo ejecuta Windows XP, Windows Me o Windows 2000, MSI ya existe en el sistema. Si el equipo ejecuta una versión anterior de Windows, puede que ya tenga MSI si instaló con anterioridad otro software que utiliza MSI. En ambos casos, el programa de instalación mostrará el primer panel del asistente inmediatamente. Vaya al paso 5 para continuar.

   b. *Si el programa de instalación no encuentra MSI* o si hay una versión anterior de MSI instalada en el equipo, instalará los archivos necesarios para continuar con la instalación y le pedirá que reinicie el equipo. Haga clic en **Reiniciar sistema.** Cuando el equipo haya reiniciado, el programa de instalación continuará a partir del punto en que se quedó.

5. Consulte los pasos mostrados en el Asistente para la instalación de VirusScan para finalizar la instalación.

SUGERENCIA: Si el equipo no dispone de las fuentes necesarias para ver el Contrato de licencia del usuario final (CLUF), puede buscar el CLUF adecuado en el CD de instalación del software de McAfee. Debe leer y aceptar los términos del contrato para finalizar la instalación.

Utilización de McAfee VirusScan 3

Interfaz de usuario inductiva de VirusScan

Bajo la dirección de Microsoft Corporation, McAfee presenta un nuevo aspecto para McAfee VirusScan: la interfaz de usuario inductiva (IUI).

¿Qué es una interfaz de usuario inductiva?

Una IUI es parecida al diseño habitual de sitios Web: cada pantalla de la aplicación se centra en un propósito único, claramente expresado y fundamental. Una IUI también permite desplazarse con facilidad de una pantalla a la siguiente.

¿De qué modo me ayuda una IUI?

La IUI simplifica el uso de McAfee VirusScan. En cualquier pantalla de VirusScan, puede averiguar fácilmente cómo finalizar una tarea o cómo tener acceso a otra tarea relacionada o diferente. Puede desplazarse en VirusScan con sencillez, mediante la selección de los iconos **Atrás**, **Adelante** e **Inicio**. Estos tres iconos aparecen en todas las pantallas de VirusScan.

¿Cómo se utiliza la IUI?

En primer lugar, inicie VirusScan desde el menú Inicio de Windows.

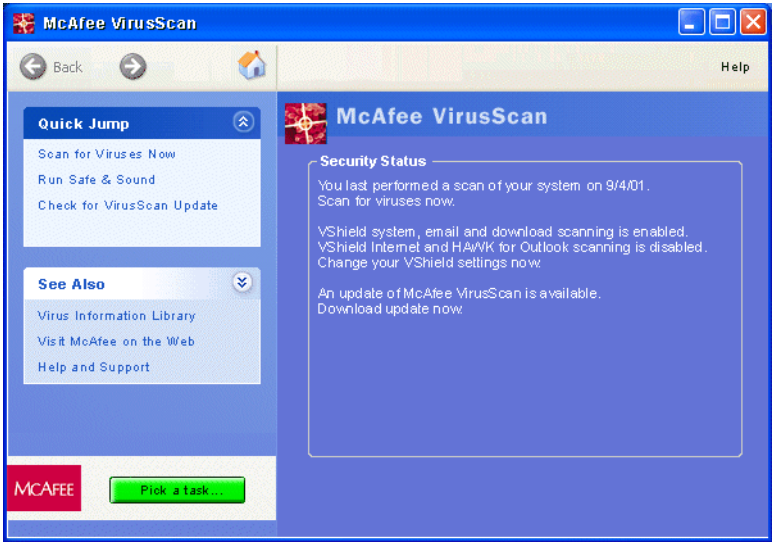


Figura 3-1. Ventana principal de VirusScan

La ventana principal de VirusScan es el punto de entrada central a todas las tareas, características y componentes de VirusScan. La ventana principal muestra tres áreas comunes a todas las pantallas de VirusScan.

Elegir una tarea

Seleccione **Elegir una tarea** para tener acceso a la pantalla principal de tareas. Desde la pantalla principal de tareas, puede seleccionar una de las tareas siguientes:

- **Explorar el equipo en busca de virus ahora**.
- **Explorar el dispositivo inalámbrico**.
- **Cambiar la configuración de VirusScan**.
- **Administrar archivos en cuarentena**.
- **Crear un disco de emergencia**.
- **Ver los registros de actividad de VirusScan**.

SUGERENCIA: Tras elegir una tarea, siga las instrucciones en línea para completarla. Si desea iniciar una nueva tarea, seleccione **Elegir una tarea**.

Avance rápido

La sección **Avance rápido** le permite tener acceso a una función o programa asociado con McAfee VirusScan (una función o programa puede contener un grupo de tareas). Por ejemplo, desde la sección Avance rápido puede:

- Seleccionar **Explorar en busca de virus ahora** para que la aplicación explore el equipo en busca de virus con las últimas opciones de configuración establecidas o con las opciones predeterminadas.
- Seleccionar **Ejecutar Safe & Sound** para mostrar la ventana de Safe & Sound y configurar las opciones de archivos de copia de seguridad.
- Seleccionar **Buscar actualización de VirusScan** para iniciar la herramienta de actualización instantánea de McAfee. La herramienta de actualización instantánea le permite descargar actualizaciones del producto, archivos de firma de virus (DAT) y el software de exploración de virus.

Consulte también

La sección **Consulte también** muestra vínculos a recursos externos para ayudarle a utilizar McAfee VirusScan. Desde la sección Consulte también puede:

- Seleccionar **Biblioteca de información sobre virus** para iniciar el navegador de Internet e ir al sitio Web de McAfee A.V.E.R.T. (Anti-Virus Emergency Response Team). Aquí encontrará información actualizada acerca de virus conocidos y de sus síntomas y podrá descargar actualizaciones de los archivos DAT.
- Seleccionar **McAfee en el Web** para iniciar el navegador de Internet e ir a www.McAfee-at-Home.com. Nuestro sitio Web McAfee-at-Home es un recurso de gran valor para todas las necesidades de soporte técnico de McAfee VirusScan.
- Seleccionar **Ayuda y soporte** para mostrar la Ayuda en línea. Elija Temas de ayuda del menú Ayuda para ver una lista de los temas de ayuda de VirusScan.

SUGERENCIA: Haga clic en la **X** de la esquina superior derecha de cualquier ventana de VirusScan para cerrar la ventana principal de VirusScan.

Uso del explorador de VShield

El explorador de VShield dispone de funciones únicas que hacen que sea una parte fundamental del completo paquete de seguridad de software antivirus VirusScan. Estas funciones incluyen:

- **Exploración automática**: Esto significa que el explorador busca virus en los archivos que se abren, copian, guardan o modifican de cualquier otra forma, así como en los que se leen o escriben en disquetes o unidades de red. Por consiguiente, puede detectar y detener los virus en el momento en que aparecen en el sistema, incluidos los que llegan a través de correo electrónico o como descargas de Internet. Esto significa que puede hacer que el explorador de VShield sea tanto la primera línea de defensa antivirus, como la protección de respaldo entre cada operación de exploración que realice. El explorador de VShield detecta virus en la memoria y cuando intentan ejecutarse desde archivos infectados.
- **Funcionamiento automático**: El explorador de VShield se integra con una amplia gama de software de navegación y aplicaciones cliente de correo electrónico. El explorador de VShield se inicia cuando arranca el equipo y permanece en memoria hasta que lo apaga o apaga el sistema.
- **Detección y bloqueo de objetos perjudiciales**: El explorador de VShield puede evitar que los objetos ActiveX y Java perjudiciales tengan acceso al sistema, antes de que se conviertan en una amenaza. Para ello, explora los cientos de objetos que se descargan durante una conexión con el Web u otros sitios Internet y los archivos adjuntos que se reciben con el correo electrónico. Después, compara estos elementos con una lista actualizada de objetos perjudiciales y bloquea los que pueden causar problemas.
- **Filtro de sitios de Internet**: El explorador de VShield se distribuye con una lista de sitios Web o Internet peligrosos que suponen una amenaza para el sistema, normalmente en forma de software perjudicial descargable. Puede agregar cualquier otro sitio al que no quiera que se conecte el software de navegación, ya sea incluyendo su dirección de Protocolo de Internet (IP) o su nombre de dominio.

Propiedades de exploración de VShield

El explorador de VShield se compone de cinco módulos relacionados, cada uno con una función especializada. Puede configurar las opciones de estos módulos en el cuadro de diálogo Propiedades de VShield. Los módulos de VShield son:

- **Exploración de sistema.** Este módulo busca virus en el disco duro mientras trabaja con su equipo. Realiza un seguimiento de los archivos a medida que el sistema u otros equipos leen archivos del disco duro o escriben archivos en él. También puede explorar disquetes y unidades de disco asignadas al sistema.
- **Exploración del correo electrónico.** Este módulo explora mensajes de correo electrónico y datos adjuntos a los mensajes que recibe a través de sistemas de correo electrónico entre oficinas y a través de Internet. Explora los sistemas de buzón de correo de Microsoft Exchange y Outlook. Funciona en conjunción con el módulo Exploración de transferencias para explorar correo de Internet que se recibe a través de Simple Mail Transfer Protocol (SMTP, protocolo de transferencia de correo simple) o Post Office Protocol (POP-3, protocolo de oficina de correos).
- **Exploración de transferencias.** Este módulo explora los archivos que descarga en el sistema desde Internet. Si ha activado la opción Correo de Internet en el módulo Exploración del correo electrónico, esto incluirá los datos y archivos adjuntos al correo electrónico que reciba a través de sistemas de correo electrónico SMTP o POP-3, lo que incluye programas cliente de correo electrónico como Eudora Pro, Microsoft Outlook Express, correo de Netscape y correo de America Online.
- **Filtro de Internet.** Este módulo busca y bloquea la descarga y ejecución en el sistema de clases Java y controles ActiveX hostiles mientras visita sitios de Internet. También puede evitar que el navegador se conecte a sitios de Internet potencialmente peligrosos que albergan software perjudicial.
- **Hostile Activity Watch Kernel (HAWK).** HAWK supervisa el equipo para buscar actividad sospechosa que pueda indicar que el sistema tiene un virus. Al contrario que VirusScan, que limpia el virus, HAWK evita que los virus, gusanos y caballos de Troya se propaguen.
- **Seguridad.** Este módulo ofrece protección mediante contraseña para los demás módulos de VShield. Puede proteger alguna o todas las páginas de propiedades de los módulos individuales y establecer una contraseña para evitar cambios no autorizados.

SUGERENCIA: Para mostrar la ventana Propiedades de VShield, haga clic con el botón derecho del ratón en el icono de VShield que aparece en la bandeja del sistema de Windows, señale Propiedades y seleccione el módulo de VShield que desea ver.

Cómo iniciar y detener el explorador de VShield

Siga los pasos que se describen a continuación para iniciar y detener el explorador de VShield.

1. Con VShield en ejecución, desde la barra de tareas de Windows, seleccione Inicio > Configuración > Panel de control.
   Aparece el Panel de control de Windows.
2. Haga doble clic en el icono de VirusScan.
   Aparece el cuadro de diálogo Servicios de VirusScan.
3. Seleccione la ficha Servicio y haga clic en Detener.
   El explorador de VShield se detiene.

SUGERENCIA: Puede iniciar o reiniciar el explorador de VShield mediante los pasos descritos más arriba.

El explorador de VShield está configurado para iniciarse automáticamente cada vez que se inicie el equipo. Para evitar que el explorador de VShield se ejecute al iniciar, quite la marca de la casilla de verificación **Cargar al iniciar**.

¿Qué debería hacer si se detecta un virus?

En primer lugar, no se asuste. Aunque están lejos de ser inofensivos, algunos de los virus que infectan a su PC o dispositivo inalámbrico pueden destruir datos o inutilizarlos.

Pueden interferir con el funcionamiento normal de su equipo o su dispositivo inalámbrico y también pueden tener otros efectos no deseados. Debe tomarlos en serio y asegurarse de eliminarlos cuando los encuentre.

McAfee VirusScan le facilita la tarea de tratar los virus cuando los detecta. A través de un cuadro de diálogo de mensaje de alerta, se presentan opciones que puede llevar a cabo sólo con seleccionar el curso de acción deseado.

Cuando McAfee VirusScan detecta un virus, aparece un mensaje de alerta que lo informa y le ofrece opciones para que decida cómo desea proceder.

Las siguientes opciones se encuentran disponibles:

- Haga clic en **Limpiar** si desea que McAfee VirusScan limpie el archivo infectado.
- Haga clic en **Eliminar** si desea que McAfee VirusScan elimine el archivo.

- Haga clic en **Continuar** si desea que McAfee VirusScan no lleve a cabo ninguna acción y que continúe explorando otros archivos.
- Haga clic en **Cuarentena** para aislar el archivo infectado de los demás archivos, programas y unidades del equipo.
- Haga clic en **Detener** para finalizar todos los procesos en ejecución.
- Haga clic en **Más información**... si desea obtener información adicional acerca del virus encontrado.

Uso de Hostile Activity Watch Kernel (HAWK)

Hostile Activity Watch Kernel (HAWK, núcleo de vigilancia de actividad hostil) es una opción de VirusScan que permite la supervisión constante de actividad sospechosa que puede indicar que hay un virus en el sistema. La actividad sospechosa incluye:

- Un intento de reenviar correo electrónico a una gran parte de su libreta de direcciones.
- Intentos muy seguidos de reenviar varios mensajes de correo electrónico.
- Datos adjuntos al correo electrónico que contienen archivos de programa (archivos ejecutables con la extensión de archivo .exe) o secuencias de comandos que pueden utilizarse para enmascarar el tipo real del documento transmitido.

Aunque VirusScan realiza muy bien la tarea de detectar virus conocidos, no puede detectar virus nuevos sin una actualización del archivo DAT. Al supervisar estas actividades típicamente perjudiciales, HAWK lo informa y le permite actuar antes de que se causen daños. HAWK puede evitar que los virus, los gusanos y los caballos de Troya se propaguen mientras VirusScan limpia el virus para eliminarlo del equipo.

Uso de Cuarentena

Muchos componentes de VirusScan permiten mover los archivos infectados a una carpeta de cuarentena. Con ello, los archivos infectados se retiran de las áreas donde están accesibles y el usuario puede limpiarlos o borrarlos cuando le resulte conveniente.

Administración de archivos en cuarentena

Esta lista describe las opciones disponibles para administrar archivos en cuarentena:

- **Agregar.** Seleccione esta opción para buscar y poner en cuarentena un archivo sospechoso.
- **Limpiar.** Seleccione esta opción para eliminar el código de virus del archivo infectado. Si no es posible eliminar el virus, se informará al usuario en su área de mensajes.
- **Restablecer.** Seleccione esta opción para devolver un archivo a su ubicación original.

ADVERTENCIA: Esta opción no limpia el archivo. Asegúrese de que el archivo no está infectado antes de seleccionar Restaurar.

- **Eliminar.** Seleccione esta opción para eliminar el archivo infectado. Asegúrese de anotar la ubicación del archivo para tener un registro de los archivos eliminados. Para restaurar los archivos eliminados deberá utilizar las copias de seguridad.
- **Enviar a McAfee.** Seleccione esta opción para enviar los virus nuevos a McAfee.

NOTA: McAfee se ha comprometido a proporcionar herramientas eficaces y actualizadas que puede utilizar para proteger su sistema. Para ello, le invitamos a que nos informe de cualquier nuevo virus, clase Java, control ActiveX o sitio Web peligroso que VirusScan no detecte actualmente.

Si ha encontrado algo que sospecha puede tratarse de un virus nuevo o no identificado, envíe el archivo infectado al equipo de emergencia (Anti-Virus Emergency Response Team) de McAfee Labs para su análisis, utilizando para ello el Asistente Enviar a McAfee. Tiene la opción de eliminar sus datos personales del archivo antes de enviarlo.

Network Associates se reserva el derecho a utilizar cualquier información que envíe de la manera que considere más adecuada, sin por ello incurrir en obligación alguna.

- **Propiedades.** Seleccione esta opción para ver las características del archivo en cuarentena. Las características incluyen, por ejemplo: tipo de archivo, tamaño, origen del archivo (no del posible virus), etc.

- **Actualizar.** Seleccione Actualizar para actualizar los detalles de los archivos que aparecen en la lista de archivos en cuarentena.

Uso de VirusScan en un dispositivo inalámbrico

El crecimiento continuo de la demanda de dispositivos inalámbricos acarrea consigo la posibilidad de poner en peligro sus datos ante la amenaza de virus, especialmente en los casos en que intercambia información entre su PC y su dispositivo inalámbrico.

Los dispositivos inalámbricos que ofrece el mercado hoy en día están diseñados fundamentalmente para funcionar como alternativas prácticas para el almacenamiento y la recuperación de datos, tales como actividades personales, direcciones de contactos, números de teléfono, citas, gastos, etc. Ya sea en el trabajo o en casa, puede llevar registros de todas esas áreas de manera sencilla mediante el uso de su dispositivo inalámbrico. Incluso puede establecer una alarma que le avise de reuniones, eventos o tareas importantes durante el día, la semana o el mes.

McAfee VirusScan es una aplicación diseñada para proteger sus datos mediante la exploración de los archivos de su dispositivo inalámbrico cada vez que se lleva a cabo un intercambio de datos o una actualización con su equipo. Protege al sistema de los virus que se pudieran haber guardado en el dispositivo inalámbrico durante el uso de características como las transferencias por infrarrojo y las transacciones inalámbricas. McAfee VirusScan es compatible con la mayoría de dispositivos inalámbricos que utilizan los sistemas operativos Palm OS ®, Pocket PC, Windows ® CE ® y EPOC (consulte la tabla siguiente).

Tabla 3-1. Ejemplos de dispositivos inalámbricos compatibles con McAfee VirusScan

Sistema operativo	Dispositivo inalámbrico	Fabricante
Palm OS ®	• Palm ™ Handheld	Palm, Inc.
	• Palm ™ VII Series	
	• Palm ™ V Series	
	• Palm ™ III Series Palm ™ M Series	
	• Visor ™	HandSpring
	• Visor Edge ™	
	• Clie	Sony
Pocket PC	• E-115	Casio

Tabla 3-1. Ejemplos de dispositivos inalámbricos compatibles con McAfee VirusScan

Sistema operativo	Dispositivo inalámbrico	Fabricante
	• iPAQ	Compaq
	• iPAQ H3600 Series	
	• Aero	
	• Aero 2100 Series	
	• PPT 2700 Series	Symbol Technologies
	• Jornada 540	Hewlett-Packard
	• Jornada 680	
	• Jornada 720	
	• E125	Cassiopeia
	• EM500	
Windows ® CE ®	• PenCentra 130	Fujitso
	• HPW-600 ET	Hitachi
	• WorkPad z50	IBM
EPOC	• Psion Series 5MX	Psion PLC
	• Psion - Revo	
	• Mako	Diamond

Sincronización de datos

La sincronización de datos es una característica estándar de la mayoría de los sistemas operativos inalámbricos que permite la sincronización de información o registros entre un dispositivo inalámbrico y un equipo de escritorio. Esta característica se conoce habitualmente, según el tipo de dispositivo que utilice, como: HotSync ® para dispositivos con Palm OS; ActiveSync para Pocket PC y Windows CE; y Psion Synchronizer para dispositivos con EPOC.

Por ejemplo, si agrega una entrada nueva en la Lista de direcciones de su dispositivo inalámbrico, la misma entrada se agrega automáticamente a la plataforma de su PC tras efectuar una sincronización de datos. Para reducir el tiempo que lleva completar la sincronización de datos en ambas plataformas, sólo cambia los datos modificados, actualizados o agregados.

Cuando se efectúa una operación de intercambio de datos, debe ejecutarse un administrador de sincronización de datos (por ejemplo: HotSync Manager, ActiveSync o Psion Synchronizer). Ésta es la aplicación que hace posible la operación de sincronización de datos. Controla su equipo y responde ante cualquier comando relacionado con la sincronización de datos cuando se inicia desde el dispositivo inalámbrico.

NOTA: Dependiendo del sistema operativo de su dispositivo inalámbrico, consulte "Requisitos adicionales para dispositivos inalámbricos", en la página 16 para determinar el tipo y la versión del administrador de sincronización de datos (por ejemplo: HotSync Manager, ActiveSync) que debe tener para poder utilizar McAfee VirusScan.

VirusScan analiza los datos transmitidos entre el equipo y el dispositivo inalámbrico durante la sincronización de datos. Si VirusScan detecta la presencia de datos infectados, el usuario puede tratar el archivo infectado del mismo modo en que trataría cualquier otro archivo infectado. Para obtener más información acerca de este tema, consulte "¿Qué debería hacer si se detecta un virus?", en la página 24.

VirusScan para Palm OS ®

Acerca de Palm OS ®

Palm OS ®, desarrollado por Palm, Inc., es uno de los tipos de sistemas operativos más habituales utilizados para dispositivos informáticos inalámbricos. Está diseñado específicamente para la administración de información móvil. A través de un dispositivo inalámbrico, puede tener acceso fácilmente a información personal o comercial sincronizada en cualquier momento y, lo que es más importante, en cualquier lugar.

Uno de sus componentes más importantes es la tecnología de sincronización del conducto de datos HotSync ®, que le permite intercambiar información entre su dispositivo inalámbrico y su equipo de escritorio.

McAfee VirusScan para Palm OS ® explora su dispositivo en busca de virus antes de que se pueda descargar en su equipo. Utiliza un componente en su PC y un componente en el dispositivo para explorar el dispositivo durante una operación de HotSync ® con su PC.

Inicio de los componentes antivirus de Palm

Puntee el icono de McAfee VirusScan para Palm OS ®. En su dispositivo aparecen varios botones de opción de casillas de verificación. Estas opciones son:

- Explorar al iniciar HotSync.
- Explorar al terminar HotSync.
- Explorar las aplicaciones.
- Explorar los datos de las aplicaciones.
- Registros modificados solamente.
- Tipos de archivos conocidos solamente.
- Tipos de ejecutables conocidos solamente.
- Explorar memoria flash.

Opciones disponibles en el componente del dispositivo

Las opciones disponibles en el componente del dispositivo inalámbrico le permiten personalizar el funcionamiento de McAfee VirusScan en los componentes de su dispositivo. La selección de la opción que más necesita ayudará a optimizar la protección y el tiempo de exploración.

NOTA: Si cambia opciones en el componente de la aplicación del dispositivo o de su PC, se modificarán ambos componentes al sincronizar. Los únicos archivos que se exploran son los que van a través del conducto hacia y desde el dispositivo.

- Explorar al iniciar HotSync.
  Esta opción le permite explorar archivos al iniciar HotSync ®.
- Explorar al terminar HotSync.
  Esta opción explora archivos al terminar HotSync ®.
- Explorar las aplicaciones.
  Esta opción le permite explorar sus aplicaciones.
- Explorar los datos de las aplicaciones.
  Esta opción le permite explorar los datos de sus aplicaciones.
- Registros modificados solamente.
  Esta opción le permite explorar únicamente los registros de datos que se modificaron desde la última operación de HotSync ®.

- Tipos de archivos conocidos solamente.
  Esta opción le permite explorar únicamente los archivos de base de datos conocidos.
- Tipos de código ejecutable conocido solamente.
  Esta opción le permite explorar únicamente los archivos ejecutables conocidos.
- Explorar memoria flash.
  Esta opción le permite explorar únicamente la memoria flash de su dispositivo inalámbrico para detectar la presencia de virus.

SUGERENCIA: Puede seleccionar cualquier combinación de las opciones de exploración anteriores.

Opciones disponibles en el componente de PC

NOTA: Para una protección antivirus total, McAfee VirusScan requiere que el componente de PC se instale en el equipo con el que sincronizará el dispositivo inalámbrico. No podrá explorar el dispositivo en busca de virus si el componente de PC de McAfee VirusScan no está instalado.

Las opciones disponibles en el componente de PC le permiten personalizar el funcionamiento de McAfee VirusScan. La selección de la opción que más necesita ayudará a optimizar la protección y el tiempo de exploración.

Opciones de Qué explorar

- Explorar las aplicaciones.
  Esta opción le permite explorar las aplicaciones transferidas al dispositivo.
- Explorar los datos de las aplicaciones.
  Esta opción le permite explorar los datos de las aplicaciones transferidos al dispositivo.
- Registros modificados solamente.
  Esta opción le permite explorar únicamente los registros de datos transferidos al dispositivo que se modificaron desde la última operación de HotSync ®.
- Tipos de archivos conocidos solamente.
  Esta opción le permite explorar únicamente los archivos de base de datos conocidos transferidos al dispositivo.
- Tipos de código ejecutable conocido solamente.
  Esta opción le permite explorar únicamente los archivos ejecutables conocidos transferidos al dispositivo.

- Explorar memoria flash.
  Esta opción le permite explorar la memoria flash de su dispositivo inalámbrico para detectar la presencia de virus.

NOTA: Puede seleccionar cualquier combinación de las opciones de exploración anteriores.

Opciones de Cuándo explorar

Las siguientes son otras opciones disponibles que le permitirán optimizar aún más el funcionamiento de McAfee VirusScan en su dispositivo inalámbrico.

- Al comienzo de cada HotSync.
  Esta opción le permite explorar su dispositivo inalámbrico en busca de virus al comienzo de cada HotSync ®.
- Al final de cada HotSync.
  Esta opción le permite explorar su dispositivo inalámbrico en busca de virus al terminar cada HotSync ®.

Otras opciones

Después de seleccionar la configuración de exploración, puede elegir cualquiera de las siguientes opciones:

- Haga clic en Aceptar para aceptar los cambios en la configuración de exploración y actualización.
- Haga clic en Cancelar para ignorar los cambios y cerrar la ventana.

Cómo eliminar McAfee VirusScan para los componentes de Palm OS ®

Siga los pasos que se describen a continuación para eliminar McAfee VirusScan de los componentes del dispositivo.

1. En la ventana principal de la aplicación, puntee el reloj.
2. En el menú Aplicación, elija Eliminar.
3. Seleccione McAfee VirusScan en el menú y, a continuación, puntee el botón Eliminar.
4. Puntee Sí en la ventana Eliminar aplicación.
5. Puntee Listo para cerrar la pantalla.

SUGERENCIA: Si elimina accidentalmente McAfee VirusScan de su dispositivo Palm, encontrará un archivo de copia de seguridad en el directorio de copias de seguridad de su Palm. Este archivo se encuentra normalmente en Palm \"nombreusuario"\Backup \PalmAV.PRC, aunque si busca PalmAV.PRC, también encontrará el archivo. Cuando encuentre el archivo, haga doble clic en él para agregarlo a la Herramienta de instalación de Palm. La próxima vez que efectúe una operación de HotSync ® con su dispositivo, McAfee VirusScan estará restaurado.

VirusScan para Windows ® CE ® y Pocket PC

NOTA: Las características y funciones asociadas a McAfee VirusScan para Windows ® CE ® funcionan de modo similar a las de Pocket PC. Esta sección es aplicable a ambos sistemas operativos.

Acerca de Windows ® CE ®

Windows ® CE ® de Microsoft ® es una plataforma de sistema operativo que ofrece una amplia gama de dispositivos de comunicaciones, entretenimiento y computación móvil. Una de sus características principales es la capacidad de compartir información con equipos basados en Windows. Es un sistema operativo compacto y portátil que se utiliza en una gran variedad de dispositivos de comunicaciones, como PC inalámbricos, localizadores digitales de información y teléfonos celulares inteligentes.

Para obtener más información acerca de productos inalámbricos que utilizan Windows ® CE ®, visite su sitio Web en www.pocketpc.com.

Acerca de Pocket PC

Los dispositivos Pocket PC no sólo organizan información. Además de la capacidad de vincular información con su equipo a la perfección, también le permiten leer mensajes de correo electrónico y explorar el Web. Los fabricantes de este tipo de dispositivo inalámbrico incluyen compañías como Hewlett Packard, Casio Computer Co., Ltd. y Compaq. Para ver ejemplos de dispositivos inalámbricos Pocket PC, visite www.pocketpc.com.

Opciones disponibles en el componente de PC

Las opciones disponibles en el componente de PC le permiten personalizar el funcionamiento de McAfee VirusScan con su dispositivo. La selección de las opciones que más necesita ayudará a optimizar la protección y el tiempo de exploración.

Opciones de Qué explorar

- Explorar todos los archivos.
  Esta opción le permite explorar todos los archivos de su dispositivo inalámbrico.
- Sólo archivos de programa.
  Esta opción le permite explorar únicamente los archivos que utiliza con mayor frecuencia su dispositivo inalámbrico.
- Archivos nuevos o modificados solamente.
  Esta opción le permite explorar únicamente los registros de datos que se modificaron o crearon desde la última operación de exploración.
- Explorar archivos marcados como in-ROM.
  Esta opción le permite explorar archivos marcados actualmente como “in-ROM”.

Opciones de Cuándo explorar

Las siguientes son otras opciones disponibles que le permitirán optimizar aún más el funcionamiento de McAfee VirusScan en su dispositivo inalámbrico.

- Explorar cada vez que un dispositivo CE se conecte a su PC.
  Esta opción le permite explorar cualquier dispositivo Windows ® CE ® o Pocket PC que sincroniza con su equipo de escritorio.

Otras opciones

Después de seleccionar la configuración de exploración, puede elegir cualquiera de las siguientes opciones:

- Haga clic en Aceptar para aceptar los cambios en la configuración de exploración y actualización.
- Haga clic en Cancelar para ignorar los cambios y cerrar la ventana.
- Haga clic en Actualizar ahora para efectuar una comprobación manual de actualizaciones de archivos de firma antivirus.
- Haga clic en Explorar ahora para iniciar una exploración de virus en su dispositivo inalámbrico.

VirusScan para EPOC de Symbian

Acerca de EPOC

Symbian es una compañía que desarrolla sistemas operativos inalámbricos móviles. Utiliza el sistema operativo EPOC, capaz de ofrecer aplicaciones y comunicaciones en un pequeño paquete (es decir: dispositivos inalámbricos). Para obtener más información, visite el sitio Web de la compañía en www.symbian.com.

Opciones disponibles en el componente de PC

Las opciones disponibles en el componente de PC le permiten personalizar el funcionamiento de McAfee VirusScan con su dispositivo. La selección de la opción que más necesita ayudará a optimizar la protección y el tiempo de exploración.

Opciones de Qué explorar

- Explorar todos los archivos.
  Esta opción le permite explorar todos los archivos de su dispositivo inalámbrico.
- Sólo archivos de programa.
  Esta opción le permite explorar únicamente los archivos que utiliza con mayor frecuencia su dispositivo inalámbrico.
- Archivos nuevos o modificados solamente.
  Esta opción le permite explorar únicamente los registros de datos que se modificaron o crearon desde la última operación de exploración.

Opciones de Cuándo explorar

Las siguientes son otras opciones disponibles que le permitirán optimizar aún más el funcionamiento de McAfee VirusScan en su dispositivo inalámbrico.

- Explorar cada vez que un dispositivo EPOC se conecte a su PC.
  Esta opción le permite explorar cualquier dispositivo EPOC que sincroniza con su equipo de escritorio.
- Cerrar todos los programas en el dispositivo EPOC antes de explorar.
  Esta opción le permite cerrar programas antes de efectuar una exploración de virus.

Otras opciones

Después de seleccionar la configuración de exploración, puede elegir cualquiera de las siguientes opciones:

- Haga clic en Aceptar para aceptar los cambios en la configuración de exploración y actualización.
- Haga clic en Cancelar para ignorar los cambios y cerrar la ventana.
- Haga clic en Actualizar ahora para efectuar una comprobación manual de actualizaciones de archivos de firma antivirus.
- Haga clic en Explorar ahora para iniciar una exploración de virus en su dispositivo inalámbrico.

NOTA: Si desea conocer la versión del software de exploración y de los archivos de firma antivirus (DAT) que McAfee VirusScan utiliza para detectar problemas en su dispositivo inalámbrico, haga clic en Acerca de. Este cuadro de diálogo también muestra fechas que le permitirán determinar la necesidad de actualizar los archivos DAT para asegurar la máxima protección antivirus de su dispositivo inalámbrico.

Utilización de Safe & Sound

Safe & Sound es una utilidad de copia de seguridad única que crea automáticamente copias de seguridad de sus documentos a medida que va trabajando con ellos.

Puede configurar Safe & Sound para que realice la copia de seguridad en una unidad diferente, a través de una conexión de red o en un área protegida de la unidad local (c:\).

Si sus archivos resultan dañados a causa de un virus, si el sistema se bloquea o si pierde sus archivos, la utilidad Safe & Sound de McAfee le proporciona la capacidad de recuperar los archivos mediante la utilidad de recuperación Safe & Sound de Windows o DOS.

Cómo crea Safe & Sound copias de seguridad automáticas

Cuando se elige que Safe & Sound cree automáticamente un conjunto de copias de seguridad, el primer conjunto se crea mientras se ejecuta el asistente de Safe & Sound. A partir de ese momento, mientras la opción Activar copia de seguridad automática esté seleccionada, continúa actualizando el conjunto de copias de seguridad en el intervalo de tiempo especificado. Si opta por crear copias de seguridad de espejo, Safe & Sound actualizar el conjunto de copias de seguridad al mismo tiempo que se vuelven a guardar los archivos originales.

Definición de la estrategia de copia de seguridad

Cuando haya decidido qué tipo de copia de seguridad desea utilizar (archivo de volumen protegido o directorio), las preguntas más importantes a las que debe responder a la hora de definir su propia estrategia de copia de seguridad son las siguientes:

¿Dónde se almacenará el conjunto de copias de seguridad?

En el mercado informático actual, puede descubrir que es igual de rentable adquirir un disco duro de copia de seguridad independiente donde puede guardar una copia de seguridad de espejo actual de una o más unidades que utilice en su PC.

Además, puede que desee almacenar la copia de seguridad en una ubicación remota para aumentar la protección. Siempre que Safe & Sound pueda tener acceso a la unidad lógica asignada a su PC, puede almacenar en ella el conjunto de copias de seguridad. Es decir, este conjunto puede guardarse en una unidad de red compartida.

¿Qué archivos son importantes (qué archivos deben copiarse)?

Safe & Sound selecciona automáticamente los archivos que suelen ser importantes para incluirlos en un conjunto de copias de seguridad. Sin embargo, puede seleccionar otros archivos o tipos de archivos para incluirlos en este conjunto.

¿Con qué frecuencia debe el usuario o Safe & Sound realizar estas copias de seguridad?

Cuanto más reciente sea su conjunto de copias de seguridad más se alegrará cuando su PC tenga algún problema que ponga en peligro los datos de las unidades principales. Sin embargo, puede que desee mantener el retraso de escritura predeterminado de 20 minutos para dar tiempo a recuperar una versión anterior de un archivo si alguna vez lo necesita.

Configuración de Safe & Sound

El asistente para la configuración de Safe & Sound le guía a través de la configuración inicial. Consulte la ayuda en línea para obtener más información acerca de la configuración de Safe & Sound.

Siga los pasos que se describen a continuación para obtener acceso a la ayuda en línea de Safe & Sound.

1. Inicie Safe & Sound desde el menú Inicio de Windows.
   Aparece la interfaz de Safe & Sound.
2. Haga clic en Ayuda.
   Aparece la ventana Ayuda de Safe & Sound.
3. Haga clic en Temas de ayuda.
   Aparece la ficha Contenido de la ventana Temas de ayuda: Safe & Sound.
4. Seleccione el tema de ayuda que desee.
5. Haga doble clic en el tema de ayuda o haga clic en Mostrar para ver el contenido del tema de ayuda.

Creación de discos de emergencia

Mientras se instala, el software VirusScan examina la memoria del equipo y los sectores de arranque del disco duro para comprobar que puede copiar los archivos en el disco duro sin riesgo de infectarse. Durante la instalación, el programa de instalación ofrece la posibilidad de crear un disco de emergencia que puede utilizarse para iniciar el sistema en un entorno libre de virus. Si el software VirusScan puede resultar infectado o si desea estar seguro de que el equipo está libre de virus antes de instalar cualquier otro software, cree y utilice un disco de emergencia para iniciar el equipo.

El software VirusScan incluye un asistente para la creación de discos de emergencia que hace que la creación de discos sea sencilla y rápida.

El disco de emergencia creado incluye BOOTSCAN.EXE, un explorador de la línea de comandos especializado y de huella pequeña que puede explorar los sectores de arranque del disco duro y el Registro de arranque principal (MBR). BOOTSCAN.EXE funciona con un conjunto especial de archivos de definición de virus (.DAT) diseñados para buscar virus en el sector de arranque. Si ya ha instalado el software VirusScan con las opciones de instalación predeterminadas, encontrará estos archivos .DAT en la siguiente ubicación en el disco duro:

C:\Archivos de programa\Archivos comunes\McAfee VirusScan\VirusScan Engine\4.0.xx

Los archivos .DAT especiales se denominan:

- EMCLEAN.DAT
- EMNAMES.DAT
- EMSCAN.DAT

McAfee actualiza periódicamente estos archivos .DAT para detectar nuevos virus del sector de arranque. Puede descargar archivos .DAT de emergencia actualizados desde la siguiente ubicación:

http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/tools.asp

NOTA: McAfee recomienda que descargue los nuevos archivos .DAT de emergencia directamente en un disquete al que se haya dado formato para reducir el riesgo de infección.

Cómo eliminar infecciones 4

Descripción general

Aunque no son inocuos, la *mayoría* de los virus que pueden infectar su equipo no destruyen datos, introducen bromas ni dejan el equipo inutilizable. Incluso los comparativamente escasos virus que llevan una carga útil destructiva sólo liberan sus efectos dañinos en respuesta a un evento desencadenador. En la mayoría de los casos, salvo que realmente tenga pruebas de que se ha activado una carga útil, dispondrá de tiempo suficiente para tratar correctamente la infección. No obstante, la mera presencia de estos pequeños fragmentos de código informático no deseado pueden interferir en el funcionamiento normal del equipo, consumir recursos del sistema o tener otros efectos no deseados, por lo que debe tomarlos en serio y asegurarse de que los elimina si los encuentra.

Una segunda idea que es preciso tener en cuenta es que el comportamiento extraño del equipo, las caídas inexplicables del sistema y otros sucesos impredecibles pueden tener una causa distinta de la infección vírica. Si cree que puede tener un virus en el equipo debido a problemas como los anteriores, es posible que la exploración no dé los resultados esperados, pero le ayudará a eliminar una posible causa de los problemas del equipo.

La medida más segura que puede adoptar es instalar el software VirusScan y explorar el sistema inmediata y minuciosamente.

Cuando instala el software VirusScan, el programa de instalación inicia la aplicación VirusScan para examinar la memoria del equipo y los sectores de arranque del disco duro y comprobar así que puede copiar sus archivos de modo seguro al disco duro sin riesgos de que se infecten. Si la aplicación no detecta ninguna infección, continúe con la instalación y explore el sistema minuciosamente cuando reinicie el equipo. Puede que los virus que infectan archivos y que no se cargan en la memoria del equipo ni se esconden en los bloques de arranque del disco duro se encuentren en algún lugar del sistema.

Cómo eliminar las infecciones detectadas durante la instalación

SUGERENCIA: Siga los pasos que se describen a continuación si se detecta una infección y desea realizar una limpieza minuciosa del equipo.

Si la aplicación VirusScan detecta un virus durante la instalación, tendrá que eliminarlo del sistema antes de instalar el programa. Para aprender cómo hacerlo, consulte los pasos que se describen a continuación.

IMPORTANTE: Para asegurar un nivel máximo de seguridad, también debería seguir estos mismos pasos si un componente de VirusScan detecta un virus en la memoria del equipo en algún momento después de la instalación.

Si el software VirusScan encontró una infección durante la instalación, siga estos pasos atentamente:

1. Salga de la instalación inmediatamente y apague el equipo.

   Asegúrese de que el equipo está desconectado. *No* presione CTRL+ALT+SUPR ni reinicie el equipo para reiniciar el sistema. Algunos virus permanecen intactos durante este tipo de reinicio “en caliente”.

2. Si creó un disco de emergencia de VirusScan durante la instalación, proteja el disco contra escritura e introduzca el mismo en la unidad de disquetes. (Ver SUGERENCIA.)

SUGERENCIA: El CD de instalación de VirusScan contiene una versión del disco de emergencia en forma de CD de ejecución automática. Si no creó un disco de emergencia *y* el equipo está configurado para iniciarse con un CD de ejecución automática, introduzca el CD de instalación de VirusScan en la unidad de CD-ROM antes de pasar al siguiente paso.

3. Espere 15 segundos como mínimo; a continuación, vuelva a iniciar el equipo.

   Mientras se reinicia el equipo, el disco de emergencia ejecuta un archivo por lotes que le dirige a través de una operación de exploración de emergencia. El archivo por lotes le pregunta primero si apagó el equipo antes de reiniciar.

4. Escriba **y** para continuar; a continuación vaya al paso 7 en la página 44. En caso negativo, escriba n, apague el equipo completamente y vuelva a empezar.

   El archivo por lotes le indica que va a iniciar una operación de exploración.

5. Lea el mensaje que aparece en pantalla y, a continuación, presione cualquier tecla para continuar.

El disco de emergencia cargará los archivos que necesita en la memoria. Si el equipo posee memoria extendida, cargará los archivos de la base de datos en esta memoria, para una ejecución más rápida.

BOOTSCAN.EXE, el explorador de la línea de comandos incluido en el disco de emergencia, realizará cuatro exploraciones para examinar los sectores de arranque del disco duro, el Registro de arranque principal (MBR), los directorios del sistema, los archivos de programa y otros posibles puntos de infección en todos los discos duros del equipo local.

NOTA: McAfee le aconseja que no interrumpa el explorador BOOTSCAN.EXE mientras ejecuta la operación de exploración. El disco de emergencia no detecta virus de macro, virus script ni programas de caballo de Troya, pero detecta virus comunes que infectan archivos y el sector de arranque.

Si BOOTSCAN.EXE encuentra un virus, intentará limpiar el archivo infectado. Si no puede hacerlo, denegará el acceso al archivo y continuará con la operación de exploración. Después de finalizar todas las exploraciones, aparece en la pantalla un informe de resumen de las acciones que se realizaron para cada disco duro. El informe indica:

- El número de archivos que el explorador examinó.
- Cuántos de esos archivos están limpios o no están infectados.
- El número de archivos que contienen posibles infecciones.
- Cuántos de esos archivos limpió el explorador.
- El número de archivos del sector de arranque y del MBR que el explorador examinó.
- El número de archivos del sector de arranque y del MBR que contienen posibles infecciones.

Si el explorador detecta un virus, emite un tono e indica el nombre y la ubicación del virus en la pantalla.

6. Cuando el explorador haya terminado la examinación del disco duro, extraiga el disco de emergencia de la unidad de disquetes y vuelva a apagar el equipo.

7. Cuando BOOTSCAN.EXE haya terminado de examinar el sistema, puede:

   - **Volver a trabajar en el equipo.** Si BOOTSCAN.EXE no encontró ningún virus o si limpió todos los archivos infectados que encontró, extraiga el disco de emergencia de la unidad de disquetes y reinicie el equipo. Si pensaba instalar el software VirusScan en el equipo pero interrumpió el proceso cuando el programa de instalación encontró una infección, puede continuar con la instalación.
   - **Tratar de limpiar o eliminar los archivos infectados.** Si BOOTSCAN.EXE encontró un virus que no pudo eliminar, identificará los archivos infectados y le indicará que no puede limpiarlos o que no dispone del limpiador adecuado para ese virus concreto.

   Como paso siguiente, ubique y elimine el archivo o archivos infectados. En este caso, tendrá que recuperar los archivos borrados desde archivos de copia de seguridad. Compruebe también si los archivos de copia de seguridad contienen virus. Asimismo, utilice la aplicación VirusScan en cuanto pueda para explorar el sistema y asegurarse de que no tiene virus.

Cómo eliminar una infección en Windows

Cuando McAfee VirusScan detecta un virus, aparece un mensaje de alerta en la pantalla para avisarle. La mejor medida que puede adoptar es intentar limpiar el archivo infectado. La limpieza elimina el virus de su PC o dispositivo inalámbrico y repara el archivo infectado.

Si **Limpiar** no elimina el virus de su PC o dispositivo inalámbrico, existen otros métodos de eliminación de virus disponibles.

1. **Eliminar** el archivo. Al hacer clic en Eliminar, tanto el virus como el archivo infectado se eliminan del equipo.

SUGERENCIA: Elija Eliminar ***sólo*** si dispone de una copia de seguridad del archivo.

---

2. Seleccione **Cuarentena** para aislar el archivo infectado. Cuando haya puesto en cuarentena el archivo infectado, utilice la función de actualización instantánea para descargar archivos de firma de virus actualizados. A continuación, intente limpiar el archivo infectado de nuevo.

   También puede intentar obtener un antídoto de A.V.E.R.T.

3. Si aún así no consigue eliminar el virus, seleccione **Detener** para detener la exploración y utilice el método de reparación del disco de emergencia descrito en la sección anterior – "Cómo eliminar las infecciones detectadas durante la instalación".

Actualización del producto de McAfee 5

Actualización instantánea

A medida que las tecnologías avanzan, proporcionamos continuamente actualizaciones de los productos de software de McAfee. Para asegurar el máximo nivel de protección, debería obtener siempre la última versión de su producto de McAfee.

La actualización del software es sencilla gracias a la función de actualización instantánea de McAfee. Es un proceso sin problemas y requiere una interacción mínima por parte del usuario.

IMPORTANTE: La actualización instantánea es también el mecanismo utilizado para registrar su producto con McAfee. Para obtener actualizaciones del producto, debe registrarlo con McAfee.

¿Por qué debe realizar la actualización?

- Puede que se incluyan nuevas características en su producto de McAfee
- Periódicamente, hay disponibles mejoras del producto
- El producto se actualiza periódicamente con contenido nuevo
- Las actualizaciones de archivos de firma de virus están disponibles con frecuencia

¿Cómo funciona el proceso de actualización?

La actualización instantánea le permite obtener y aplicar actualizaciones de sus productos de McAfee mientras está conectado a Internet. Si existe una actualización, recibirá una notificación. En ese mismo momento, puede descargar y aplicar las actualizaciones de sus productos.

Características de la actualización instantánea

- **Consulta automática.** Si activa esta opción, recibirá notificaciones de actualizaciones del producto mientras está conectado a Internet. La configuración predeterminada de la actualización instantánea es tener esta opción activada. Si no se conecta a Internet con frecuencia, es aconsejable que desactive esta opción y utilice la característica de actualización manual.

SUGERENCIA: Le recomendamos que no tenga la opción de consulta automática activada si tiene una conexión lenta a Internet.

- **Actualización automática.** Si no desea recibir mensajes de notificación acerca de actualizaciones, puede activar la opción de actualización automática. Si activa esta opción, podrá descargar y aplicar actualizaciones del producto sin recibir mensajes de notificación. Las actualizaciones se descargan y se aplican “silenciosamente” a su producto de McAfee.
- **Actualización manual.** Si casi nunca se conecta a Internet, la opción más adecuada es utilizar la actualización manual con su producto de McAfee. Puede realizar la actualización manual mientras está conectado a Internet. Para ello, seleccione la función ACTUALIZAR desde el producto individual.

SUGERENCIA: La actualización manual le proporciona control explícito del proceso de actualización.

Configuración

Para obtener información adicional acerca de la configuración de la consulta automática y la actualización automática, consulte la ayuda en línea.

Soporte al producto A

ANTES DE PONERSE EN CONTACTO CON McAfee Software para obtener soporte técnico, sitúese cerca del equipo en el que se ha instalado el producto de McAfee y compruebe la siguiente información:

- Número de versión del software de McAfee

> **SUGERENCIA:** Desde la ventana principal de McAfee VirusScan, seleccione Ayuda > Acerca de para encontrar esta información.

- Número de versión del sistema operativo Windows
- Capacidad de memoria (RAM)
- Descripción completa del problema
- Mensaje de error EXACTO que aparece en pantalla
- ¿Qué pasos realizó antes de recibir el mensaje de error?
- Si el error es persistente, ¿puede reproducir el problema?
- Nombre del modelo de disco duro (interno o externo)
- Tarjetas, placas o hardware adicional

Cómo ponerse en contacto con McAfee

Network Associates International B.V.
P.O. Box 58326
1040 HH Amsterdam
Países Bajos
Tel.: +(31) 20 586 6100

McAfee Customer Service
Laan van de Leeuw
7324 BD Apeldoorn
Países Bajos
Fax: +31 (0) 55 543 4646

www.McAfee-at-Home.com

McAfee es famoso por el buen trato que profesa a sus clientes. Para conservar esta tradición, hemos convertido nuestro sitio en el World Wide Web en un valioso recurso para obtener respuestas a sus preguntas acerca de los productos de McAfee. Le animamos a que nos visite en *http://www.mcafee-at-home.com* y lo convierta en la primera parada para todas sus necesidades de soporte al producto.

NOTA: Para obtener información acerca del estado de un pedido existente, envíe un mensaje de correo electrónico a *support_retail_es@nai.com*.

Cómo ponerse en contacto con el Soporte técnico

Para obtener soporte asistido, visite *http://www.mcafeehelp.com*. Nuestro sitio Web de soporte ofrece acceso las 24 horas del día a las soluciones a las peticiones de soporte más habituales en nuestro sencillo Asistente para respuestas en tres pasos. Asimismo, también puede utilizar nuestras opciones avanzadas, que incluyen una búsqueda por palabra clave y el árbol de ayuda, diseñadas para los usuarios más expertos. Si no encuentra solución a su problema, también puede tener acceso a nuestras opciones GRATUITAS Email Express! y Chat Now!, que funcionan 24 horas al día. Estas opciones le permitirán ponerse en contacto rápidamente con nuestros ingenieros de soporte cualificados, a través de Internet y sin costo alguno. La información de soporte telefónico también puede obtenerse desde nuestro sitio Web de autoayuda en: *http://www.mcafeehelp.com*.

Foros de soporte y contacto telefónico

Si no encuentra lo que necesita, pruebe uno de nuestros servicios automatizados en una de las siguientes ubicaciones.

World Wide Web	*www.mcafee-at-home.com*
Comercio electrónico	*http://estore.nai.com*
Sitio Web de soporte	*http://www.mcafeehelp.com*
Sitio Web de descargas	*http://www.mcafee-at-home.com/download/default.asp*
CompuServe	*GO MCAFEE*
America Online	*palabra clave MCAFEE*
Microsoft Network	*mcafee*

Índice

W

Para obtener más información acerca de productos, servicios internacionales y soporte técnico, póngase en contacto con su representante autorizado de ventas de McAfee o visítenos en:

www.mcafee-at-home.com

MCAFEE

A Network Associates Business

NA-518-0010-SP-1