McAfee VirusScan

Guía del usuario

COPYRIGHT

Copyright © 2000 Network Associates, Inc. y sus Sociedades afiliadas. Reservados todos los derechos. Ninguna parte de esta publicación se puede reproducir, transmitir, transcribir, almacenar en un sistema de copia de seguridad o traducir a otro idioma de ninguna forma, ni por ningún medio, sin permiso por escrito de Network Associates, Inc.

ATRIBUCIONES DE MARCAS COMERCIALES

** ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, CNX, Compass 7, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, GroupShield, HelpDesk, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee, McAfee Associates, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetOctopus, NetRoom, NetScan, Net Shield, NetShield, NetStalker, Net Tools, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, Pop-Up, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey- International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, Switch PM, TeleSniffer, TIS, TMach, TMeg, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, T-POD, Trusted Mach, Trusted Mail, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall* y *ZAC 2000* son marcas registradas de Network Associates y sus empresas afiliadas en los Estados Unidos u otros países. Todas las demás marcas registradas y sin registrar que aparecen en este documento son propiedad exclusiva de sus respectivos propietarios.

ACUERDO DE LICENCIA

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL SIGUIENTE ACUERDO LEGAL ("ACUERDO"), PARA LA LICENCIA DEL SOFTWARE ESPECIFICADO ("SOFTWARE") POR PARTE DE NETWORK ASSOCIATES, INC. ("McAfee"). AL HACER CLIC EN EL BOTÓN ACEPTAR O INSTALAR EL SOFTWARE, USTED (COMO PERSONA FÍSICA O PERSONA JURÍDICA) SE COMPROMETE A ACEPTAR EL ACUERDO Y A CONVERTIRSE EN UNA DE SUS PARTES INTEGRANTES. SI NO ESTÁ DE ACUERDO CON ALGUNA DE LAS CONDICIONES DE ESTE ACUERDO, HAGA CLIC EN EL BOTÓN QUE INDICA QUE NO ACEPTA SUS TÉRMINOS Y NO INSTALE EL SOFTWARE (SI ES APLICABLE, PUEDE DEVOLVER EL PRODUCTO AL LUGAR DONDE LO ADQUIRIÓ A EFECTOS DE OBTENER UN REEMBOLSO ÍNTEGRO).

1. **Concesión de licencia.** Sujeto al pago de la tarifa correspondiente a la licencia y a las condiciones y términos especificados en este Acuerdo, McAfee por la presente concede al usuario el derecho no exclusivo e intransferible a utilizar una copia de la versión especificada del Software y la documentación adjunta ("Documentación"). Puede instalar una copia del Software en un equipo, estación de trabajo, ayudante digital personal, localizador, "teléfono inteligente" u otro dispositivo electrónico para el que se haya diseñado el Software (constituyendo cada uno un "Dispositivo Cliente"). Si se concede una licencia del Software como conjunto de programas con más de un producto de Software especificado, esta licencia se aplica a todos los productos de Software

especificados, sujeta a las limitaciones o condiciones de uso especificadas individualmente para cada uno de los productos de Software en la lista de precios aplicable o en la caja.

a. **Uso.** Se concede licencia del Software como un único producto, no se puede utilizar en más de un Dispositivo Cliente o por más de un usuario cada vez, excepto en los casos que se establecen en la Sección 1. El Software está "en uso" en un Dispositivo Cliente cuando se carga en la memoria temporal (es decir, en la memoria de acceso aleatorio o RAM) o se instala en la memoria permanente (por ejemplo, en el disco duro, un CD-ROM u otro dispositivo de almacenamiento) de ese Dispositivo Cliente. Esta licencia le autoriza a realizar una copia del Software únicamente como copia de seguridad o para archivo, siempre y cuando la copia contenga todos los avisos de propiedad del Software.

b. **Uso en un servidor.** Puede utilizar el Software en un Dispositivo Cliente como un servidor ("Servidor") dentro de un entorno de red o de varios usuarios ("Uso en un servidor") sólo si la lista de precios aplicable o la caja del producto así lo indican. Es necesaria una licencia diferente para cada Dispositivo Cliente o puesto que se pueda conectar al Servidor en cualquier momento, independientemente de que los Dispositivos Cliente o puestos se conecten, accedan o utilicen el Software simultáneamente. El uso de software o hardware que reduzca el número de Dispositivos Cliente o puestos que acceden directamente al Software o lo utilizan (por ejemplo, hardware o software "multiplexing" o "pooling") no reduce el número de licencias requeridas (es decir, debe disponer de un número de licencias igual al número de accesos diferentes realizados al software o hardware multiplexing o pooling). Si el número de Dispositivos Cliente o puestos que se pueden conectar al Software puede exceder el número de licencias que usted ha obtenido, deberá disponer de un mecanismo razonable que garantice que el uso del Software no excederá los límites de uso establecidos para las licencias que ha obtenido. Esta licencia le autoriza a realizar o descargar una copia de la Documentación para cada uno de los Dispositivos Cliente o puestos que disponen de licencia, siempre y cuando las copias contengan los avisos de propiedad de la Documentación.

c. **Licencias de volumen.** Si la licencia del Software incluye condiciones de licencia de volumen especificadas en la lista de precios o en la caja del producto, puede realizar, utilizar e instalar tantas copias adicionales del Software para el número de Dispositivos Cliente como autorice la licencia de volumen. Debe disponer de un mecanismo razonable que garantice que el número de Dispositivos Cliente en los que se ha instalado el software no excede el número de licencias que ha obtenido. Esta licencia le autoriza a realizar o descargar una copia de la Documentación para cada una de las copias adicionales autorizadas por la licencia de volumen, siempre y cuando las copias contengan los avisos de propiedad de la Documentación.

2. **Duración.** Este Acuerdo tiene vigor durante un periodo de tiempo ilimitado a menos que finalice antes por cualquiera de las condiciones que se describen a continuación. Este Acuerdo termina automáticamente si usted no cumple alguna de las limitaciones o requisitos descritos en este documento. Una vez terminado el acuerdo o dada por finalizada su vigencia, debe destruir todas las copias del Software y la Documentación. Puede dar por terminado este Acuerdo en cualquier momento mediante la destrucción de todas las copias del Software y de la Documentación.

3. **Actualizaciones.** Durante el periodo de tiempo especificado en la lista de precios o en la caja del producto aplicable para el Software, tiene derecho a descargar revisiones o actualizaciones del Software tan pronto como McAfee las incluya en su sistema de boletín electrónico, sitio web u otros

servicios en línea. Durante un periodo de noventa (90) días a partir de la fecha de compra original del Software, tiene derecho a descargar una (1) revisión o ampliación del Software tan pronto como McAfee la incluya en su sistema de boletín electrónico, sitio web u otros servicios en línea. Una vez transcurrido el periodo de tiempo especificado, no tendrá derecho a recibir ninguna revisión o ampliación sin adquirir previamente una nueva licencia o contratar un plan anual de actualización para el Software.

4. **Derechos de propiedad.** El Software está protegido por las leyes de copyright de Estados Unidos y por las disposiciones de los tratados internacionales. McAfee y sus proveedores son los propietarios y retienen todo derecho, título e interés referente al Software, incluidos todos los copyrights, patentes, derechos de secreto de fabricación, marcas comerciales y todos los derechos de propiedad intelectual que impliquen. La posesión, instalación o uso del Software no le concede ningún título sobre la propiedad intelectual del Software y no adquirirá ningún derecho sobre el Software excepto los que se establecen en este Acuerdo. Las copias del Software y de la Documentación contendrán los mismos avisos de propiedad que aparecen en el Software y en la Documentación.

5. **Limitaciones.** No puede alquilar, arrendar, prestar o revender el Software. No puede permitir que terceros se beneficien del uso o funcionalidad del Software mediante un acuerdo de multipropiedad, de oficina de servicios o de cualquier otro tipo, con la excepción de lo especificado de otro modo en la lista de precios aplicable o en la caja del producto. No puede transferir los derechos que se le han otorgado en virtud de este Acuerdo. No puede utilizar técnicas de ingeniería inversa, descompilación ni desensamblaje del Software, excepto en el caso de que la legislación aplicable prohiba expresamente la limitación anterior. El usuario no puede modificar ni crear ningún trabajo derivado del Software completo o de parte de éste. No puede copiar el Software o la Documentación excepto en los casos expresamente permitidos en la Sección 1. No puede quitar ningún aviso o etiqueta sobre la propiedad del Software. McAfee se reserva todos los derechos no especificados expresamente de aquí en adelante. McAfee se reserva el derecho de realizar auditorías periódicas, avisando por escrito con antelación, para verificar el cumplimiento de los términos de este Acuerdo.

6. **Garantía y renuncia**

   a. **Garantía limitada.** McAfee garantiza que durante los sesenta (60) días siguientes a la fecha de la adquisición original, los medios de distribución (por ejemplo, discos) en que se incluye el Software estarán libres de defectos en materiales y fabricación.

   b. **Soluciones para el cliente.** La única responsabilidad de McAfee y sus distribuidores, y el único recurso que le compete a usted será, a juicio de McAfee, (i) la devolución del precio de compra pagado por la licencia, si la hubiera, o bien (ii) la sustitución del medio defectuoso que contiene el Software. Debe devolver el medio defectuoso a McAfee, corriendo usted con los gastos, junto con una copia del recibo. Esta limitación de garantía no tiene efecto si el defecto se debe a accidente, abuso o mal uso. Cualquier medio de sustitución estará garantizado por el resto del período original de garantía. Fuera de Estados Unidos, este recurso no está disponible en la medida en que McAfee está sujeto a las leyes y reglamentos de exportación de Estados Unidos.

c. **Renuncia de garantía.** Con excepción de la garantía limitada que se especifica más adelante en el presente documento, EL SOFTWARE SE PROPORCIONA "TAL CUAL". EN LA MEDIDA PERMITIDA POR LA LEY APLICABLE, MCAFEE RENUNCIA A CUALQUIER OTRA GARANTÍA, EXPRESA O IMPLÍCITA, INCLUYENDO, AUNQUE NO DE FORMA EXCLUSIVA, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN DETERMINADO FIN Y AUSENCIA DE INFRACCIÓN CON RESPECTO AL SOFTWARE Y A LA DOCUMENTACIÓN QUE LO ACOMPAÑA. USTED ASUME LOS RIESGOS Y RESPONSABILIDADES QUE EMANAN DE LA SELECCIÓN DEL SOFTWARE CON EL FIN DE LOGRAR LOS RESULTADOS DESEADOS, ASÍ COMO DE LA INSTALACIÓN, USO Y RESULTADOS OBTENIDOS DEL SOFTWARE. SIN LIMITAR LAS DISPOSICIONES ANTERIORES, MCAFEE NO OTORGA NINGUNA GARANTÍA DE QUE EL SOFTWARE ESTÉ LIBRE DE ERRORES, INTERRUPCIONES U OTROS FALLOS, NI DE QUE EL SOFTWARE SATISFARÁ SUS EXIGENCIAS. PUESTO QUE ALGUNOS ESTADOS Y JURISDICCIONES NO PERMITEN LIMITACIONES DE GARANTÍAS IMPLÍCITAS, LA LIMITACIÓN ANTERIOR PUEDE NO SER APLICABLE A SU CASO. Las disposiciones anteriores sólo serán exigibles en la medida en que lo permita la legislación aplicable.

7. **Limitación de responsabilidad.** EN NINGUNA CIRCUNSTANCIA Y BAJO NINGUNA TEORÍA LEGAL, YA SEA EXTRACONTRACTUAL, CONTRACTUAL O SIMILAR, SERÁ RESPONSABLE MCAFEE O SUS PROVEEDORES ANTE USTED U OTRA PERSONA POR NINGÚN DAÑO DIRECTO O INDIRECTO DE CUALQUIER ÍNDOLE INCLUYENDO, AUNQUE NO DE FORMA EXCLUSIVA, LOS DAÑOS DERIVADOS DE LA PÉRDIDA DE FONDOS, INTERRUPCIÓN DEL FUNCIONAMIENTO, FALLO O MAL FUNCIONAMIENTO DEL EQUIPO, NI POR NINGÚN OTRO DAÑO O PÉRDIDA. EN NINGÚN CASO SERÁ RESPONSABLE MCAFEE DE LOS DAÑOS POR EXCESO DEL PRECIO QUE MCAFEE COBRA POR UNA LICENCIA PARA EL SOFTWARE, INCLUSO SI HABÍA AVISADO A MCAFEE DE LA POSIBILIDAD DE TALES DAÑOS. ESTA LIMITACIÓN DE RESPONSABILIDAD NO SE APLICA A LA RESPONSABILIDAD POR MUERTE O DAÑOS A PERSONAS EN LA MEDIDA EN QUE LA LEGISLACIÓN APLICABLE PROHIBA TAL LIMITACIÓN. ADEMÁS, ALGUNOS ESTADOS Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LIMITACIÓN DE DAÑOS DIRECTOS O INDIRECTOS, POR LO QUE PUEDE QUE ESTA LIMITACIÓN Y EXCLUSIÓN NO SEAN APLICABLES A SU CASO. Las disposiciones anteriores sólo serán exigibles en la medida en que lo permita la legislación aplicable.

8. **Gobierno de Estados Unidos.** El Software y la Documentación que lo acompaña se consideran "commercial computer software (software informático comercial)" y "commercial computer software documentation (documentación de software informático comercial)", respectivamente conforme a lo estipulado en la sección 227.7202 de DFAR y en la sección 12.212 de FAR, como sea aplicable. El uso, modificación, reproducción, publicación, ejecución, visualización o divulgación del Software y de la Documentación que lo acompaña por el Gobierno de Estados Unidos se regirá únicamente por los términos de este Acuerdo y estará prohibido excepto en la medida en que expresamente lo permitan los términos de este Acuerdo.

9. **Controles de exportación.** Ni el Software ni la Documentación ni la información o tecnología subyacente se pueden descargar ni exportar o reexportar (i) a (o a un ciudadano o residente de) Cuba, Irán, Iraq, Libia, Corea del Norte, Sudán, Siria o cualquier otro país al que Estados Unidos haya embargado bienes; ni (ii) a nadie que se encuentre en la lista de naciones designadas especialmente del Departamento del Tesoro de Estados Unidos o de la tabla de órdenes de denegaciones del Departamento de Comercio de Estados Unidos. Al descargar o utilizar el Software, usted acepta las disposiciones anteriores y certifica que no se encuentra en ninguno de estos países ni listas, ni bajo el control de los mismos y que tampoco es ciudadano o residente de tales países.

   ADEMÁS, DEBE ESTAR AL TANTO DE LO SIGUIENTE: LA EXPORTACIÓN DEL SOFTWARE PUEDE ESTAR SUJETA AL CUMPLIMIENTO DE NORMAS Y REGLAMENTOS PROMULGADOS DE VEZ EN CUANDO POR LA OFICINA DE EXPORTACIÓN DEL DEPARTAMENTO DE COMERCIO DE ESTADOS UNIDOS, QUE LIMITAN LA EXPORTACIÓN Y REEXPORTACIÓN DE DETERMINADOS PRODUCTOS Y DATOS TÉCNICOS. SI LA EXPORTACIÓN DEL SOFTWARE ESTÁ CONTROLADA POR NORMAS Y REGLAMENTOS, NO SE PODRÁ EXPORTAR NI REEXPORTAR EL SOFTWARE, DIRECTA O INDIRECTAMENTE, (A) SIN TODAS LAS LICENCIAS DE EXPORTACIÓN Y REEXPORTACIÓN Y LA APROBACIÓN DEL GOBIERNO DE ESTADOS UNIDOS U OTRO GOBIERNO QUE REQUIERA LA LEGISLACIÓN APLICABLE, O (B) SI ELLO SUPUSIESE LA VIOLACIÓN DE ALGUNA PROHIBICIÓN APLICABLE A LA EXPORTACIÓN O REEXPORTACIÓN DE CUALQUIER PARTE DEL SOFTWARE.

   ALGUNOS PAISES TIENEN LIMITACIONES SOBRE EL USO DE CODIFICACIÓN DENTRO DE SUS FRONTERAS, O SOBRE LA IMPORTACIÓN O EXPORTACIÓN DE CODIFICACIÓN INCLUSO SI ES SÓLO PARA UN USO PERSONAL O COMERCIAL TEMPORAL. USTED RECONOCE QUE LA IMPLEMENTACIÓN Y CUMPLIMIENTO DE ESTAS LEYES NO ES SIEMPRE COHERENTE RESPECTO A PAISES ESPECÍFICOS. AUNQUE LA SIGUIENTE LISTA DE PAÍSES NO ES EXHAUSTIVA, PUEDE HABER LIMITACIONES SOBRE LA EXPORTACIÓN O IMPORTACIÓN DE CODIFICACIÓN EN: BÉLGICA, CHINA (INCLUIDO HONG KONG), FRANCIA, INDIA, INDONESIA, ISRAEL, RUSIA, ARABIA SAUDÍ, SINGAPUR Y COREA DEL SUR. USTED RECONOCE QUE ES SU RESPONSABILIDAD CUMPLIR LA LEGISLACIÓN GUBERNAMENTAL SOBRE EXPORTACIÓN Y OTRAS LEYES APLICABLES, Y QUE MCAFEE NO TIENE RESPONSABILIDAD ALGUNA DESPUÉS DE LA VENTA INICIAL ANTE USTED DENTRO DEL PAÍS DE VENTA ORIGINAL.

10. **Actividades de alto riesgo.** El Software no es tolerante a errores y no está diseñado ni pensado para utilizarlo en entornos peligrosos que requieran una ejecución de alta seguridad, incluyendo, aunque no de forma exclusiva, el funcionamiento en instalaciones nucleares, sistemas de comunicación o navegación para aeronaves, control del tráfico aéreo, sistemas de armamento, máquinas de mantenimiento directo de la vida humana o cualquier otra aplicación en la que el fallo del software podría producir directamente la muerte, daños a las personas o graves daños materiales o de la propiedad (colectivamente denominados "Actividades de alto riesgo"). McAfee renuncia de manera expresa a toda garantía implícita o explícita de idoneidad para Actividades de alto riesgo.

11. **Varios.** Este Acuerdo se rige por las leyes de Estados Unidos y el estado de California, sin hacer referencia a conflictos de principios de leyes. La aplicación de la Convención de Naciones Unidas sobre contratos para la venta internacional de bienes está expresamente excluida. Este Acuerdo establece todos lo derechos del Software para el usuario y representa el acuerdo completo entre las partes. Este acuerdo sustituye cualquier otra comunicación con respecto al Software y la Documentación. Este Acuerdo no se puede modificar excepto por un apéndice escrito por un representante debidamente autorizado de McAfee. Ninguna disposición del presente documento se considerará no aplicable a menos que exista una exención por escrito y firmada por McAfee o un representante debidamente autorizado de McAfee. Si se considera no válida alguna disposición de este Acuerdo, el resto del Acuerdo continuará en plena vigencia. Las partes confirman que es su deseo que este Acuerdo se escriba en español únicamente.
12. **Servicio de atención al cliente de McAfee.** Si tiene alguna pregunta en relación con estos términos y condiciones o si desea ponerse en contacto con McAfee por cualquier otro motivo, llame al 901 11 67 32, envíe un fax al +31 (0) 55 543 4646, o escriba a: McAfee Software Division, P.O. Box 898, 7301 BC Apeldoorn, Paises Bajos. http://www.mcafee.com.

    Las manifestaciones realizadas durante el curso de esta venta están sujetas a la ley sobre disponibilidad e información del año 20000, Year 2000 Information and Readiness Disclosure Act (Public Law 105-271). En caso de disputa, esta ley puede reducir sus derechos legales referentes al uso de cualquier manifestación sobre la disponibilidad para el año 2000, a menos que se especifique otra cosa en el contrato o en la lista de precios.

Tabla de contenido

Prefacio xiii
¿Qué ha ocurrido? xiii
¿Por qué preocuparse? xiii
¿De dónde proceden los virus? xiv
Antecedentes de los virus xv
Los virus y la revolución de los equipos informáticos xv
En el límite xix
¿Qué es lo siguiente? xxi
Cómo protegerse xxii

Capítulo 1. Acerca del software de VirusScan 25
Introducción al software antivirus VirusScan 25
¿Cómo funciona el software de VirusScan? 28
¿Qué incluye el software de VirusScan? 31
Novedades de esta versión 36

Capítulo 2. Instalación del software de VirusScan 39
Antes de comenzar 39
Requisitos del sistema 39
Otras recomendaciones 39
Preparación para instalar el software de VirusScan 40
Opciones de instalación 40
Pasos de instalación 40
Uso de la utilidad para creación del disco de emergencia 51
Determinación del momento de reiniciar el equipo 56
Comprobación de la instalación 58
Modificación o eliminación de la instalación de VirusScan 59

Capítulo 3. Eliminación de virus del sistema 61
Si sospecha que puede tener un virus 61
Cuándo explorar en busca de virus 65
Cómo reconocer que el equipo no está infectado 66

Identificación de falsas detecciones 67
Respuesta a los virus o software perjudicial 68
Envío de un ejemplo de virus 81
Uso de la utilidad SendVirus para enviar un archivo de ejemplo 81
Captura de virus del sector de arranque, infección de archivos y virus de macro 85

Capítulo 4. Utilización del explorador VShield 91
¿Qué hace el explorador VShield? 91
¿Por qué utilizar el explorador VShield? 92
Compatibilidad con visualizadores y clientes de correo electrónico 93
Activación o inicio del explorador VShield 94
Utilización del asistente de configuración de VShield 99
Definición de las propiedades del explorador VShield 104
Utilización del menú de acceso directo de VShield 159
Desactivación o detención del explorador VShield 159
Seguimiento de la información de estado del software de VShield 164

Capítulo 5. Uso de la aplicación VirusScan 167
¿Qué es la aplicación VirusScan? 167
¿Por qué utilizar la aplicación VirusScan? 168
Inicio de la aplicación VirusScan 169
Configuración de la interfaz de VirusScan en modo Clásico 174
Configurar la interfaz de VirusScan Avanzado 180

Capítulo 6. Creación y configuración de tareas programadas 199
¿Qué hace la Consola de VirusScan? 199
¿Por qué se programan las operaciones de exploración? 199
Inicio de la Consola de VirusScan 200
Utilización de la ventana de la Consola 203
Trabajar con tareas predeterminadas 205
Trabajar con la tarea VShield 206
Creación de nuevas tareas 207
Activar tareas 211

Comprobación del estado de la tarea 214
Configuración de las opciones de la aplicación VirusScan 216

Capítulo 7. Uso de herramientas de exploración especializadas 237
Exploración de correo de Microsoft Exchange y Outlook 237
¿Cuándo y por qué debe utilizarse la extensión Exploración de correo electrónico? 237
Uso de la extensión Exploración de correo electrónico 239
Configuración de la extensión Exploración de correo electrónico . . .240
Exploración de cc:Mail 257
Uso de la utilidad ScreenScan 257

Capítulo 8. Utilización de las utilidades de VirusScan 265
Descripción del panel de control de VirusScan 265
Cómo abrir el panel de control de VirusScan 266
Selección de opciones del panel de control de VirusScan 267
Utilización de la utilidad de configuración de cliente del Administrador de alertas 270
El software de VirusScan como cliente del Administrador de alertas 271
Configuración de la utilidad del cliente del Administrador de alertas 272

Capítulo 9. Acerca de Safe & Sound 277
Utilización de Safe & Sound 278
Archivo de volumen protegido (la protección de copia de seguridad definitiva) 278
Razones para realizar copias de seguridad periódicas con Safe & Sound 278
Realización de copias de seguridad automáticas con Safe & Sound 279
Definición de la estrategia de copia de seguridad 280
¿Dónde se guardará la copia de seguridad? 280
¿Cuáles son los archivos importantes? 281
¿Con qué frecuencia debe realizar el usuario o Safe & Sound estas copias de seguridad? 281

Capítulo 10. Acerca de Cuarentena 283
Utilización del componente de Cuarentena 283

Informes sobre nuevos virus u objetos 284
Envío de información sobre virus al equipo de respuesta de emergencia antivirus 284

Apéndice A. Extensiones predeterminadas de archivos comprimidos y vulnerables 287
Agregar extensiones de nombre de archivo para explorar 287
Lista actual de las extensiones de nombres de archivo vulnerables 288
Lista actual de archivos comprimidos explorados 293

Apéndice B. Servicios de soporte técnico para el producto 299
Actualizaciones 299
Cómo ponerse en contacto con McAfee 299
Servicio de atención al cliente 300
Soporte técnico 300

Apéndice C. Información para descargas (ID# de licencia: VSF500RSP) 303
SecureCast™ (para la versión comercial para Windows 95/98): 303
Acceso a Internet 303

Apéndice D. Uso del servicio SecureCast para obtener nuevos archivos de datos 305
Introducción al servicio SecureCast 305
¿Por qué se deben actualizar los archivos de datos? 306
¿Qué archivos de datos proporciona el servicio SecureCast? 307
Instalación del cliente BackWeb y del servicio SecureCast 308
Requisitos del sistema 308
Solución de problemas del servicio Enterprise SecureCast 319
Cancelación de suscripción de SecureCast 319
Recursos de soporte 320
Servicio SecureCast 320
Cliente BackWeb 320

Index 321

Prefacio

¿Qué ha ocurrido?

Si alguna vez ha perdido archivos importantes que estaban almacenados en el disco duro, ha observado con asombro cómo se apagaba el equipo para mostrar únicamente el mensaje de un bromista en el monitor o ha tenido que disculparse por tener demasiados mensajes de correo electrónico que nunca envió, ya conoce de antemano la forma en que los virus informáticos u otros programas nocivos pueden afectar a su productividad. Si nunca ha sufrido una "infección" de virus, puede estar seguro de que ha tenido suerte. Con más de 50.000 virus conocidos en circulación y capaces de atacar a los sistemas informáticos basados en DOS y en Windows, resultar afectado por un virus es sólo una cuestión de tiempo.

La ventaja es que de esos miles de virus en circulación, sólo unos pocos pueden causar daños importantes en los datos. De hecho, el término "virus informático" hace referencia a un gran número de programas que tienen una única característica en común: se "reproducen" solos de forma automática adjuntándose al software del equipo "anfitrión" o a sectores de disco del mismo, generalmente sin que el usuario lo perciba. La mayoría de los virus causan problemas irrelevantes, simplemente molestos o totalmente insignificantes. Por lo general, la principal consecuencia de una infección de virus se ve reflejada en el tiempo y esfuerzo que se invierte, ya que es necesario encontrar el origen de la infección y eliminar el rastro que han dejado a su paso.

¿Por qué preocuparse?

¿Por qué preocuparse entonces por las infecciones de virus si la mayoría de los ataques no ocasionan daños graves? El problema tiene dos aspectos: en primer lugar, aunque relativamente pocos virus tienen efectos destructivos, sí es importante el alcance de la propagación de los virus malintencionados. En muchos casos, los virus que tienen los efectos más graves son los más difíciles de detectar; el creador del virus encargado de provocar los daños toma medidas adicionales para evitar que se descubra. En segundo lugar, incluso los virus "benignos" pueden afectar al funcionamiento normal del equipo y tener consecuencias imprevisibles en otros tipos de software. Algunos virus contienen errores, códigos poco complejos u otro tipo de problemas lo suficientemente graves como para provocar interrupciones cuando se ejecutan. Otras veces, el software con licencia pueden tener problemas a la

hora de ejecutarse cuando un virus, intencionadamente o de cualquier otra forma, ha alterado los parámetros del sistema u otros elementos del entorno informático. Localizar el origen de las interrupciones o paros resultantes en el sistema puede resultar una pérdida de tiempo y dinero en detrimento de actividades más productivas.

Además de estos aspectos existe un problema de percepción: una vez infectado, el equipo pertinente puede ser el origen de infecciones de otros equipos. Si el usuario intercambia datos periódicamente con clientes o compañeros, puede pasar sin saberlo un virus que cause más daño a su reputación o a sus relaciones profesionales con otras personas que al propio equipo.

La amenaza de los virus y otros software malintencionados es real y cada vez más grave. Según algunas estimaciones, el coste total de tiempo y productividad perdida generado en todo el mundo únicamente por la detección y limpieza de infecciones de virus se eleva a 10.000 millones de dólares anuales, cifra que no incluye los costes de pérdidas y recuperación de datos en caso de que los ataques destruyan dichos datos.

¿De dónde proceden los virus?

Si un usuario se recupera de un ataque de virus o recibe información acerca de que han aparecido nuevas formas de software malintencionados en los programas más utilizados, probablemente se pregunte cómo hemos podido, en tanto que usuarios informáticos, llegar hasta tal punto. ¿De dónde proceden los virus y los programas malintencionados? ¿Quién los escribe? ¿Por qué aquellos que los escriben desean interrumpir los procesos de trabajo, destruir los datos o hacer perder a otras personas tiempo y dinero para eliminarlos? ¿Qué se puede hacer para detenerlos?

¿Por qué me ha pasado esto a mí?

Probablemente no sirva de mucho saber que ni usted ni su equipo eran el objetivo del programador que creó el virus que eliminó la tabla de asignación de archivos de su disco duro. Como tampoco servirá de ayuda saber que el problema de los virus siempre estará presente. Sin embargo, conocer a grandes rasgos la historia de los virus informáticos y la forma en que actúan puede ayudarle a protegerse más eficazmente contra ellos.

Antecedentes de los virus

Los historiadores han identificado un determinado número de programas que incluían características que ahora se asocian con los virus. El profesor e investigador canadiense Robert M. Slade establece el origen de los virus en utilidades con fines específicos que se usaban para aprovechar el espacio disponible en los archivos con el fin de realizar otras tareas útiles en los primeros equipos en red. Slade afirma que los expertos en informática de un centro de investigación de Xerox Corporation denominaron este tipo de programas "gusano", término que acuñaron al observar "agujeros" en las impresiones de mapas de memoria informáticos que parecían haber sido causados por gusanos. El término se sigue empleando actualmente para hacer referencia a los programas que realizan copias de sí mismos sin utilizar necesariamente el software host en el proceso.

Una tradición académica arraigada, que consiste en gastar bromas informáticas, fue la que probablemente contribuyó al abandono de los programas de utilidades para emplear las técnicas de programación más nocivas de los programas "gusano". Los estudiantes de informática, para demostrar sus habilidades en programación, crearon programas "gusano" malintencionados y los distribuyeron para competir entre sí y descubrir el programa que pudiera vencer a los rivales. Los mismos estudiantes también utilizaron dichos programas para gastar bromas a sus compañeros.

Algunos de estos estudiantes descubrieron muy pronto que podían utilizar determinadas características del sistema operativo del equipo "anfitrión" para obtener acceso no autorizado a sus recursos. Otros se aprovecharon de los usuarios con escasos conocimientos informáticos para sustituir utilidades comunes o inocuas por sus propios programas, creados para fines particulares. Estos usuarios poco avanzados ejecutarían lo que pensaban que era su software normal para descubrir que sus archivos habían desaparecido, que su contraseña había sido utilizada o cualquier otro tipo de consecuencias negativas. Estos programas, denominados "caballos de Troya" o "Troyas" por su parecido metafórico con el regalo griego a la antigua ciudad de Troya, siguen siendo, y cada vez más, una grave amenaza para los usuarios de hoy en día.

Los virus y la revolución de los equipos informáticos

Hoy se piensa que los primeros y verdaderos virus informáticos aparecieron, según Robert Slade, poco después de que los primeros equipos personales entraran en el mercado a principios de los años 80. Otros investigadores establecen la fecha de aparición de los programas de virus en 1986, cuando se descubrió el virus "Brain". En cualquier caso, la relación entre la amenaza de los virus y los equipos personales no es casual.

La nueva distribución masiva de equipos informáticos hizo posible que los virus contagiaran a muchos más equipos que antes, cuando sólo unos pocos sistemas mainframe, cuidadosamente supervisados, dominaban el mundo informático desde las grandes corporaciones y universidades. Los usuarios individuales que adquirían equipos informáticos tampoco tenían muchos conocimientos acerca de las sofisticadas medidas de seguridad necesarias para proteger los delicados datos en esos entornos. Como catalizador adicional, a los programadores de virus les resultó muy fácil explotar algunas tecnologías de equipos informáticos para lograr sus propios fines.

Virus de sector de arranque

Los primeros equipos, por ejemplo, "arrancaban" o cargaban sus sistemas operativos desde disquetes. Los creadores del virus Brain descubrieron que sus propios programas podían sustituir al código ejecutable existente en el sector de arranque de todos los disquetes formateados con MS-DOS de Microsoft, incluyera o no archivos del sistema. Por esta razón los usuarios cargaban los virus en la memoria cada vez que iniciaban los equipos con cualquier disquete formateado en las unidades de disquete. Una vez en la memoria, un virus puede copiarse en los sectores de arranque o en otros disquetes o discos duros. Aquellos que sin quererlo cargaban el virus Brain desde un disquete infectado, podían leer un "anuncio publicitario" de una compañía de asesoramiento de equipos en Pakistán.

Con dicho anuncio, Brain lanzó otra característica típica de los virus modernos: la carga destructiva. La carga destructiva es una broma o un comportamiento malintencionado que, al activarse, provoca efectos negativos que abarcan desde simples mensajes molestos hasta la destrucción de datos. Es la característica de los virus que más atrae la atención; muchos programadores de virus ahora los crean específicamente con el objetivo de distribuir sus cargas útiles en tantos equipos como sea posible.

Durante cierto tiempo, los sofisticados descendientes de estos primeros virus de sector de arranque representaron la amenaza más grave para los usuarios de equipos. Las variantes de los virus de sector de arranque también infectan el registro de arranque maestro (Master Boot Record, MBR), que almacena la información sobre particiones que el equipo necesita para poder encontrar cada una de las particiones del disco duro y el propio sector de arranque.

En realidad, casi todos los pasos del proceso de inicio, desde la lectura del MBR a la carga del sistema operativo, están expuestos a virus. Algunos de los virus más tenaces y destructivos todavía cuentan entre su repertorio de trucos con la habilidad de infectar el sector de inicio o el MBR. Entre otras cosas, si carga al iniciar el equipo, el virus podrá actuar antes de que se pueda ejecutar el software antivirus. Muchos productos VirusScan de McAfee.com se adelantan a esta posibilidad, al permitir crear un disco de emergencia que podrá utilizar para iniciar el equipo y eliminar las infecciones.

Sin embargo, los virus del MBR y del sector de arranque tienen un punto débil: se propagan a través de disquetes u otros medios extraíbles y permanecen ocultos en esa primera parte de espacio en disco. Puesto que hay menos usuarios que hayan intercambiado disquetes y la distribución de software se basa actualmente en otros medios, como por ejemplo los CD-ROM, otros tipos de virus han eclipsado la amenaza de los sectores de arranque. Hay que tener en cuenta que muchos virus de última generación incorporan de forma rutinaria funciones que infectan el sector de arranque del disco duro del usuario o MBR, incluso si se utilizan otros métodos como medios principales de transmisión.

Esos mismos virus se han beneficiado de varias generaciones de evolución y, por lo tanto, incorporan infecciones mucho más sofisticadas y técnicas de ocultación que hacen muy difícil su detección incluso cuando se están ocultos en lugares bastante predecibles.

Virus de infección de archivos

Al mismo tiempo, aproximadamente, que los creadores del virus Brain descubrieron la vulnerabilidad de los sectores de arranque de DOS, otros programadores de virus encontraron la forma de utilizar diferentes tipos de software para reproducir sus creaciones. Un reciente ejemplo de este tipo de virus surgió en los equipos de Lehigh University en Pennsylvania. El virus infectó parte del intérprete de comandos COMMAND.COM de DOS, que utilizaba para cargarse en la memoria. Una vez en ella, se propagaba a otros archivos COMMAND.COM cada vez que un usuario introducía un comando estándar de DOS para acceder al disco. Esto limitaba su propagación a los disquetes que incluían, por lo general, todo un sistema operativo.

Los últimos virus han superado rápidamente esta limitación, algunas veces con programaciones muy inteligentes. Los creadores de virus pueden hacer, por ejemplo, que éstos añadan su código al principio de un archivo ejecutable, de forma que cuando el usuario arranca un programa, el código del virus se ejecuta inmediatamente y, a continuación, devuelve el control al software legal, que se ejecuta como si nada hubiera pasado. Una vez activado, el virus "engancha" o "atrapa" las peticiones que el software legal envía al sistema operativo y las sustituye por sus propias respuestas.

Los virus especialmente inteligentes pueden incluso evitar ser eliminados de la memoria bloqueando la secuencia de teclas CTRL+ALT+SUPR para arrancar en caliente y, a continuación, simulando un reinicio. Algunas veces, la única indicación visible de que algo no funciona en el sistema antes de que se active la carga útil puede ser un pequeño cambio en el tamaño de los archivos del software legal infectado.

Técnicas polimórficas, de ocultación, mutación y codificación

Por pequeños que sean, los cambios en el tamaño de los archivos, así como otras señales de infección de virus, normalmente proporcionan a los software antivirus la información suficiente para localizar y eliminar el código dañino. Por lo tanto, uno de los retos principales del programador de virus es tratar de ocultar su trabajo. Los primeros disfraces eran una mezcla de programación innovadora y regalos obvios. El virus Brain, por ejemplo, desviaba las peticiones para ver el sector de arranque de un disco desde la ubicación real del sector infectado hacia la nueva ubicación de los archivos de arranque, que el virus había modificado. Esta capacidad de "ocultación" permitía a éste y otros virus evitar las técnicas de búsqueda convencionales.

Puesto que los virus tenían que evitar continuamente volver a infectar los sistemas anfitriones (al hacerlo, el tamaño del archivo infectado aumentaría de tal forma que se podría detectar fácilmente o bien utilizaría tal cantidad de recursos que resultaría muy sencillo descubrir la causa) los programadores debían también dar instrucciones a los virus para que no infectaran determinados archivos. Afrontaron este problema haciendo que los virus escribieran una secuencia de bytes característica o, en los sistemas operativos Windows de 32 bits, crear una clave de registro determinada que marcara los archivos infectados con una referencia de software equivalente a un cartel de "no molestar". Aunque esto impedía que el virus se eliminara inmediatamente, proporcionó a los programas antivirus la posibilidad de utilizar la propia secuencia de "no molestar", junto con otras secuencias características escritas por el virus en los archivos que infectaba, para averiguar cuál era la "firma de código" del virus. Actualmente, la mayoría de los proveedores de antivirus compilan y actualizan de forma regular una base de datos con "definiciones" de virus que utilizan sus productos para reconocer esas firmas de código en el archivo que exploran.

Como respuesta, los creadores de virus encontraron formas para ocultar las firmas de códigos. Algunos virus "mutaban" o transformaban sus firmas de códigos con cada nueva infección. Otros se autocodificaban y, en consecuencia, también sus firmas de códigos, dejando sólo un par de bytes para utilizar como clave de descodificación. La mayoría de los nuevos y sofisticados virus empleaban las técnicas de ocultación, mutación y codificación para aparecer con toda una variedad de formas nuevas prácticamente indetectables. Para localizar estos virus "polimórficos" era necesario que los ingenieros de software desarrollaran técnicas de programación complejas para los programas antivirus.

Virus de macro

Hacia el año 1995, la guerra de los virus atravesó una especie de tregua. Nuevos virus aparecían constantemente, en parte debido a la existencia de "paquetes" de virus ya preparados que permitían incluso a las personas sin conocimientos de programación lanzar nuevos virus en poco tiempo. No obstante, la mayoría de los programas antivirus existentes podían actualizarse fácilmente para detectar y eliminar las nuevas variedades de virus, que básicamente eran pequeñas variaciones de plantillas conocidas.

Pero el año 1995 se caracterizó por la aparición del virus Concept, que supuso un nuevo y sorprendente cambio en la historia de los virus. Antes de su aparición, los investigadores de virus pensaban que los archivos de datos (documentos de texto, hojas de cálculo y dibujo creados por el software utilizado), eran inmunes a las infecciones. Los virus, después de todo, son programas y como tales necesitan funcionar de la misma forma que lo hacen los programas ejecutables para poder causar daños. Los archivos de datos, por otra parte, simplemente almacenan la información introducida al trabajar con el software.

Esta diferencia desapareció cuando Microsoft empezó a añadir funciones de macro en Word y Excel, las aplicaciones centrales del paquete Office. Con la utilización de la versión básica del lenguaje Visual BASIC incluida en el paquete, los usuarios podían crear plantillas de documentos para formatear y añadir automáticamente otras características a los documentos creados con Word y Excel. Muy pronto otros proveedores hicieron lo mismo con sus productos, bien utilizando una variación del mismo lenguaje de macros de Microsoft o incorporando uno propio. Por otra parte, los programadores de virus aprovecharon esta oportunidad para ocultar y difundir virus en los documentos que creaba el propio usuario.

La creciente utilización de Internet y el correo electrónico, que permitía a los usuarios incluir archivos en los mensajes, favoreció la rápida y extensa propagación de los virus de macro. En el plazo de un año, los virus de macro se convirtieron en la mayor amenaza de todos los tiempos.

En el límite

Al mismo tiempo que los virus se hicieron más sofisticados y siguieron amenazando la integridad de los sistemas informáticos de los que todos habíamos llegado a depender, todavía había otros peligros que empezaron a surgir de una fuente inesperada: World Wide Web. Si bien una vez fue un depósito de documentos para investigación y de tratados académicos, este medio se ha transformado posiblemente en el más versátil y adaptable jamás inventado para las comunicaciones y el comercio.

Dado que su potencial parece tan amplio, la Web ha atraído la atención y los esfuerzos de desarrollo de prácticamente todas las empresas relacionadas con la informática.

Las convergencias tecnológicas derivadas de este enfebrecido ritmo de invenciones facilitan a los diseñadores de sitios Web herramientas que pueden utilizar para recopilar y mostrar información de formas que nunca antes habían estado disponibles. Pronto los sitios Web se difundieron tanto que fue posible enviar y recibir correo electrónico, formular y ejecutar consultas a bases de datos con sistemas de búsqueda avanzados, enviar y recibir audio y vídeo en directo y distribuir datos y recursos multimedia a personas de todo el mundo.

Mucha de la tecnología que hizo posible estas funciones disponía de pequeños programas que se descargaban fácilmente y que interactuaban con el software del visualizador y, a veces, con otro software del disco duro. Esta misma vía sirvió como punto de entrada en el sistema de otros programas menos benignos que la utilizaban para sus propios fines.

Java, ActiveX y objetos de secuencias de comandos

Estos programas, beneficiosos o dañinos, se presentan de varias formas. Algunos son aplicaciones en miniatura con una finalidad específica o "subprogramas" escritos en Java, un lenguaje de programación que desarrolló por primera vez Sun Microsystems. Otros se desarrollan con ActiveX, una tecnología de Microsoft que pueden utilizar los programadores para objetivos similares.

Tanto Java como ActiveX hacen un uso extensivo de módulos de software previamente escritos u "objetos" que los programadores pueden escribir ellos mismos o tomar de fuentes existentes para adaptarlos a aplicaciones, "subprogramas", controladores de dispositivos y demás software necesario para alimentar la Web. Los objetos Java se llaman "clases" y los objetos ActiveX se llaman "controles". La diferencia principal entre ellos está en la forma de ejecutarse en el sistema anfitrión. Las aplicaciones de Java se ejecutan en una "máquina virtual" de Java diseñada para interpretar la programación Java y traducirla en acciones en el equipo "anfitrión", mientras que los controles ActiveX se ejecutan como programas originales de Windows que vinculan y pasan datos entre otros programas de Windows.

Una inmensa mayoría de estos objetos son partes útiles, e incluso necesarias, de cualquier sitio Web interactivo. Pero a pesar de los esfuerzos de los ingenieros de Sun y Microsoft a la hora de diseñar medidas de seguridad en ellos, los programadores más decididos pueden utilizar herramientas Java y ActiveX para incluir objetos perjudiciales en los espacios Web, donde pueden ocultarse hasta que los visitantes involuntariamente les permiten vulnerar los sistemas informáticos.

A diferencia de los virus, los objetos Java y ActiveX perjudiciales normalmente no buscan la autorreproducción. La Web les proporciona multitud de oportunidades para extenderse en los sistemas informáticos objetivo, mientras que su pequeño tamaño y su naturaleza inocua hace que sea fácil que escapen a la detección. De hecho, a menos que le indique específicamente al software del visualizador que los bloquee, los objetos Java y ActiveX se descargan automáticamente en el sistema siempre que se accede a un sitio Web que los acoja.

En vez de eso, existen objetos perjudiciales que proporcionan el equivalente a la carga destructiva de un virus. Hay programadores que han escrito objetos, por ejemplo, que pueden leer datos del disco duro y enviarlos al sitio Web visitado; estos objetos pueden "secuestrar" su -cuenta de correo electrónico y enviar mensajes dañinos en su nombre, o leer los datos que se transmiten entre su equipo y otros ordenadores.

Han empezado a aparecer agentes aún más potentes en aplicaciones que se ejecutan directamente desde los sitios Web visitados. JavaScript, un lenguaje de secuencia de comandos con un nombre similar al del lenguaje Java pero sin relación con él, apareció por primera vez en Netscape Navigator, con la implementación de la versión 3.2 del estándar HTML. Desde su introducción, JavaScript ha aumentado considerablemente en cuanto a capacidad y potencia, al igual que muchas otras tecnologías que le han seguido, incluyendo Microsoft VBScript y Active Server Pages, Allaire Cold Fusion y otros. Actualmente estas tecnologías permiten que los diseñadores de software creen aplicaciones completamente comprensibles que se ejecutan en servidores Web, interactúan con bases de datos y otras fuentes de datos, y manipulan directamente funciones en el software cliente de correo electrónico y del explorador Web que se ejecutan en su equipo.

Al igual que ocurre con los objetos Java y ActiveX, existen importantes medidas de seguridad para evitar acciones perjudiciales; sin embargo, los programadores de virus y los piratas informáticos han encontrado formas de sortearlas. Los beneficios que estas innovaciones aportan a la Web, generalmente, son mayores que los riesgos, sin embargo, la mayoría de los usuarios siguen calculando si les compensa antes de rechazar estas tecnologías.

¿Qué es lo siguiente?

El software dañino ha empezado a introducirse en áreas insospechadas. Los usuarios del cliente mIRC Internet Relay Chat, por ejemplo, han encontrado virus creados a partir del lenguaje de comandos mIRC. El cliente de chat enviaba estos virus como texto normal, lo que evitaba las infecciones, pero las versiones anteriores del software cliente mIRC interpretaban las instrucciones codificadas en los procedimientos de comandos y realizaban acciones no deseadas en el equipo del destinatario.

Los distribuidores actuaron inmediatamente para deshabilitar esta capacidad en las versiones actualizadas del software, pero el caso de mIRC confirma la regla de que si existe la posibilidad de aprovechar un vacío en la seguridad del software de un programa, siempre hay alguien que lo encuentra y lo utiliza. A finales de 1999, otro programador de virus demostró que esta regla fallaba ante el virus llamado VBS/Bubbleboy que se ejecutaba directamente desde el cliente de correo electrónico de Microsoft Outlook apropiándose del soporte VBScript incorporado. Este virus sobrepasaba la marcada línea que dividía los mensajes de correo electrónico de texto normal de los archivos adjuntos susceptibles de infectarse. VBS/Bubbleboy ni siquiera necesitaba que se abriera el mensaje de correo electrónico, simplemente el hecho de verlo desde la ventana de vista preliminar de Outlook podía infectar el sistema.

Cómo protegerse

El software antivirus VirusScan de McAfee constituye una importante herramienta contra las infecciones y los daños producidos en los datos, pero es sólo parte de las medidas de seguridad que deben adoptarse como protección. Por otra parte, el software antivirus es tan bueno como lo sea su última actualización. Puesto que cada mes aparecen de 200 a 300 virus y variantes, los archivos de datos (.DAT) que hacen posible que el software McAfee VirusScan detecte y quite los virus quedan obsoletos rápidamente. Si no ha actualizado los archivos que se enviaron originalmente con el software, podría correr el riesgo de que los virus que hayan surgido recientemente infecten el sistema. Sin embargo, McAfee VirusScan Software cuenta con el personal de investigación antivirus más numeroso y experimentado del mundo en su equipo de respuesta de emergencia antivirus (AVERT)*. Esto significa que los archivos necesarios para combatir a los virus nuevos aparecen cuando se necesitan y, a menudo, antes.

La mayor parte de las demás medidas de seguridad son obvias: por ejemplo, conviene comprobar siempre los discos que tienen una procedencia desconocida o poco fiable, ya sea con un software antivirus o con cualquier otra utilidad de comprobación. Los programadores malintencionados han llegado al punto de imitar los programas en los que confía el usuario para proteger su equipo, pegando un signo familiar en el software dañino. Sin embargo, ni McAfee VirusScan ni los programas antivirus pueden detectar cuándo alguien sustituye alguna de las utilidades comerciales o compartidas en red favoritas del usuario por un caballo de Troya no identificado u otro programa perjudicial, es decir, hasta después de que haya ocurrido.

El acceso a Web o a Internet tiene su propio riesgo. El software antivirus de VirusScan* ofrece la posibilidad de bloquear sitios Web peligrosos de forma que los usuarios no puedan descargar, sin darse cuenta, software perjudicial de sitios peligrosos conocidos; además, captura objetos hostiles que se descargan de todos modos. Es necesario tener instalado un buen firewall o mecanismo de seguridad para proteger la red y poder instalar otros mecanismos de seguridad en la misma cuando existen personas sin escrúpulos que pueden introducirse en la red desde casi cualquier punto del globo, ya sea para apropiarse de datos o para introducir códigos dañinos. Debería asegurarse de que los usuarios no autorizados no tienen acceso a su red y de que dispone de un programa de formación adecuado para enseñar y hacer que se cumplan las normas de seguridad. Si desea obtener información acerca del origen, comportamiento y otras características de determinados virus, consulte la Biblioteca de información sobre virus que se encuentra en el sitio Web de AVERT.

McAfee VirusScan Software puede proporcionar al usuario otro software potente en los paquetes Active Virus Defense* (AVD) y Total Virus Defense (TVD), las soluciones antivirus más eficaces disponibles actualmente. Las empresas relacionadas con la familia de Network Associates proporcionan otras tecnologías que también contribuyen a proteger la red, incluyendo la línea de productos PGP Security CyberCop y el paquete de productos de seguimiento de redes Sniffer Technologies. Póngase en contacto con el representante de Network Associates o visite su sitio Web para obtener información sobre cómo adaptar la eficacia de estas soluciones de seguridad a sus necesidades.

Acerca del software de VirusScan 1

Es el principal punto de acceso para la utilización de todos los componentes disponibles de McAfee VirusScan. Esta pantalla inicial proporciona información como, por ejemplo, la última vez que se llevó a cabo una exploración en busca de virus en el ordenador, los parámetros de VShield que están activados o desactivados (para más información, consulte Utilización del explorador Vshield), la información DAT disponible y su fecha de creación.

Mediante esta interfaz de fácil uso puede acceder a las principales funciones de McAfee VirusScan. Haga clic en los botones correspondientes para iniciar una tarea concreta dentro de McAfee VirusScan (por ejemplo, explorar, planificar, poner en cuarentena, etc.).

Asimismo puede hacer clic en el botón Actualizar para iniciar la búsqueda y descarga de las actualizaciones disponibles para el programa McAfee VirusScan instalado en el ordenador. Compruebe que dispone de conexión a Internet antes de utilizar esta función. Para obtener más información, así como instrucciones detalladas, haga clic en el icono de ayuda situado en la esquina superior derecha de la ventana. Para ver las opciones de que dispone para personalizar los componentes de McAfee VirusScan en el ordenador, haga clic en el botón Opciones.

Introducción al software antivirus VirusScan

El ochenta por ciento de las 100 empresas con más éxito del mercado de valores de Estados Unidos (Fortune 100) y más de 50 millones de usuarios en todo el mundo eligen el software antivirus de VirusScan para proteger sus equipos contra la inmensa gama de virus y otros agentes dañinos que han aparecido en la última década, invadiendo las redes corporativas y ocasionando graves perjuicios entre los usuarios profesionales. Lo hacen porque el software de VirusScan ofrece la solución de seguridad antivirus más completa que existe actualmente para equipos individuales, con funciones que detectan virus, bloquean objetos hostiles ActiveX y Java, identifican sitios Web peligrosos, interceptan mensajes de correo electrónico que pueden infectar el equipo e incluso erradican agentes "zombi" que cooperan en ataques de retirada de servicios a gran escala a través de Internet. Lo hacen también porque reconocen el valor que la investigación y el desarrollo de antivirus de McAfee VirusScan aporta a su lucha por mantener los niveles de integridad y servicio de la red, garantizar la seguridad de los datos y reducir los costes de propiedad.

Con más de cincuenta mil virus y agentes dañinos actualmente en circulación, la importancia de esta lucha ha aumentado considerablemente. Los virus y gusanos actuales pueden ocasionar costes económicos reales en una empresa, no sólo en términos de pérdida de productividad y costes de detección y eliminación, sino también en la reducción de ingresos directos en el balance final, a medida que un mayor número de empresas realiza intercambios comerciales a través del correo electrónico y en línea y proliferan los ataques de virus.

El software de VirusScan destacó tecnológicamente por primera vez como integrante de un reducido número de utilidades pioneras desarrolladas para combatir las primeras epidemias de virus de la era de los equipos personales. Su desarrollo ha sido considerable desde entonces para hacer frente a cada nuevo subterfugio ideado por los creadores de virus. Como una de las primeras aplicaciones antivirus que tiene en cuenta Internet, actualmente conserva su valor como utilidad empresarial indispensable en la nueva economía electrónica. Ahora, con esta versión, el software de VirusScan ofrece un nivel totalmente nuevo de manejo e integración con otras herramientas antivirus de McAfee VirusScan.

Las mejoras de arquitectura significan que cada componente de VirusScan encaja perfectamente con los demás, compartiendo datos y recursos para conseguir una mejor respuesta de la aplicación y menos exigencias del sistema. La compatibilidad total con el software de administración ePolicy Orchestrator de Network Associates significa que los administradores de redes pueden manejar los detalles de configuración de componentes y tareas, con lo que podrá concentrarse en su trabajo. Por otra parte, la nueva tecnología de actualización de incrementos significa que la definición de virus y las descargas del motor de exploración pueden realizarse de forma más ágil y con menor ancho de banda; ahora la protección necesaria para hacer frente a la elevadísima velocidad con la que se distribuyen los virus de nueva generación puede llegar en menos tiempo que nunca.

La nueva versión también incluye compatibilidad con las plataformas Windows 95, Windows 98, Windows ME, Windows NT Workstation versión 4.0 y Windows 2000 Professional, todo en un único paquete con un único instalador, pero optimizado para aprovechar las ventajas que ofrece cada plataforma. Por ejemplo, los usuarios de Windows NT Workstation versión 4.0 y Windows 2000 Professional pueden ejecutar el software de VirusScan con diferentes niveles de seguridad que ofrecen una serie de opciones que los administradores del sistema deben cumplir. De esta forma, la implementación de políticas antivirus corporativas puede ser desde relativamente casual (donde un administrador pueda bloquear algunas configuraciones esenciales, por ejemplo) hasta muy estricta, con configuraciones predefinidas que los usuarios no pueden cambiar ni desactivar en modo alguno.

Al mismo tiempo, como piedra angular de los paquetes de seguridad Active Virus Defense y Total Virus Defense de McAfee VirusScan, el software de VirusScan conserva las mismas características básicas que lo han convertido en la utilidad por excelencia de los equipos que se utilizan en las empresas. Estas características incluyen una velocidad de detección de virus inigualable, funciones heurísticas eficaces, detección y eliminación de caballos de Troya, actualización rápida con versiones semanales de archivos de definición de virus (.DAT), versiones beta de archivos .DAT diarias y asistencia con archivos EXTRA.DAT en casos de crisis o epidemias de virus. Puesto que cada mes aparecen más de 300 nuevos virus o agentes de software dañinos, McAfee VirusScan respalda su software con cobertura mundial durante las 24 horas mediante su equipo de emergencia antivirus, AVERT (Anti-Virus Emergency Response Team).

Incluso con el aumento de virus y gusanos que utilizan el correo electrónico para propagarse, que inundan los servidores de correo electrónico o que infectan directamente productos de groupware (software para trabajo en grupo) y servidores de archivos, los equipos individuales siguen siendo la principal fuente de infecciones y, a menudo, el punto de entrada más vulnerable. El software de VirusScan actúa como un centinela incansable en los equipos personales; protege su sistema contra la amenaza de los virus más antiguos y contra las últimas amenazas que acechan en los sitios Web, a menudo sin el conocimiento del propietario del sitio, o que se propagan indiscriminadamente a través del correo electrónico.

En este entorno, adoptar precauciones para protegerse del software perjudicial ha dejado de ser un lujo para convertirse en una necesidad. Considere el grado de confianza que deposita en los datos del ordenador, así como el tiempo, los problemas y el dinero necesarios para sustituirlos en caso de que se corrompan o queden inservibles debido a la infección de un virus. Según algunos cálculos, los costes de detección y eliminación de virus en las empresas han alcanzado los dieciséis mil millones de dólares sólo en 1999. Compare la probabilidad de infección, y la parte de costes resultantes que su compañía tendrá que afrontar, con el tiempo y el esfuerzo necesarios para implantar algunas medidas de seguridad de sentido común, y pronto verá la utilidad de protegerse.

Aunque sus datos revistan relativamente poca importancia a nivel personal, descuidar la protección contra los virus puede llevar a que el ordenador proporcione albergue, sin su conocimiento, a un virus que podría extenderse a los equipos que utilizan sus compañeros y colegas. Si comprueba periódicamente el disco duro con el software de VirusScan, reducirá significativamente el riesgo de infección del sistema y evitará la pérdida innecesaria de tiempo, dinero y datos.

¿Cómo funciona el software de VirusScan?

El software de VirusScan combina el mejor motor de exploración del mercado de antivirus con mejoras de interfaz de primerísima categoría que proporcionan acceso completo a la potencia de ese motor. La interfaz gráfica de usuario de VirusScan unifica los componentes especializados del programa sin sacrificar la flexibilidad necesaria para adaptar el software a su entorno informático. Por otra parte, el motor de exploración combina las mejores características de las tecnologías que los investigadores de McAfee y McAfee VirusScan han venido desarrollando por separado durante más de una década.

Detección de virus rápida y precisa

La base de esa combinación la constituye el entorno de desarrollo exclusivo creada por los investigadores de McAfee VirusScan para el motor. Dicho entorno incluye Virtran, un lenguaje de programación especializado con una estructura y un "vocabulario" optimizados según las necesidades concretas de la detección de virus. Por ejemplo, utilizando funciones de biblioteca específicas de este lenguaje, los investigadores de virus pueden detectar las secciones de un archivo, de un sector de arranque o de un registro de arranque principal que los virus suelen infectar, ya sea porque pueden ocultarse en ellos o porque pueden "secuestrar" sus rutinas de ejecución. De esta forma, el explorador evita tener que examinar todo el archivo en busca de código de virus; en cambio, puede realizar un muestreo del archivo en puntos bien definidos para determinar si existen firmas de código de virus que indiquen una infección.

El entorno de desarrollo agiliza tanto la creación de archivos .DAT como las rutinas del motor de exploración. El entorno proporciona herramientas que los investigadores pueden utilizar para escribir definiciones "genéricas" que identifican familias completas de virus y que pueden detectar fácilmente decenas o cientos de variantes que componen el grueso de los nuevos virus observados. El constante perfeccionamiento de esta técnica ha trasladado la mayoría de las definiciones de virus realizadas manualmente, que solían residir en actualizaciones de archivos .DAT, directamente al motor de exploración en forma de paquetes de rutinas genéricas. Los investigadores pueden incluso emplear una función de arquitectura de Virtran para conectar nuevos "verbos" del motor que, cuando se combinan con funciones del motor existentes, pueden agregar la funcionalidad necesaria para hacer frente a nuevas técnicas de infección, nuevas variantes u otros problemas planteados por virus emergentes.

De este modo se mejoran rápidamente las posibilidades de detección del motor y se elimina la necesidad de realizar actualizaciones continuamente para detectar variantes de virus.

Detección de virus polimórficos codificados

Además de la detección de variantes de virus genéricos, el motor de exploración incorpora ahora un motor de descodificación genérica, un conjunto de rutinas que permite al software de VirusScan detectar virus que se ocultan mediante la codificación y mutación de sus firmas de código. Estos virus "polimórficos" son claramente difíciles de detectar, puesto que cambian su firma de código cada vez que se reproducen.

Esto significaba que el sencillo método de comparación de patrones utilizado anteriormente por los motores de exploración para buscar muchos virus ya no funcionaba, puesto que no existían secuencias constantes de bytes que se pudieran detectar. Para responder a esta amenaza, los investigadores de McAfee VirusScan desarrollaron el motor PolyScan Decryption Engine, que localiza y analiza el algoritmo que estos tipos de virus utilizan para su codificación y descodificación. Después ejecuta este código a través de sus recorridos en una máquina virtual emulada a fin de determinar cómo se produce la mutación de los virus. Hecho esto, el motor puede averiguar la auténtica naturaleza de estos virus y así detectarlos con seguridad, independientemente de la forma en que traten de ocultarse.

Análisis de "heurística doble"

Como mejora adicional del motor, los investigadores de McAfee VirusScan han perfeccionado las primeras tecnologías de exploración heurística, desarrolladas originalmente para detectar la avalancha de variantes de virus de macro que aparecieron a partir de 1995, para convertirlas en un conjunto de herramientas de precisión. Las técnicas de exploración heurística se basan en la experiencia del motor con virus anteriores para predecir la posibilidad de que un archivo sospechoso sea un nuevo virus aún sin identificar o clasificar.

Ahora, el motor de exploración incorpora ViruLogic, una técnica heurística que puede observar el comportamiento de un programa y evaluar en qué medida se parece a un virus de macro *o* a un virus de infección de archivos. ViruLogic busca comportamientos similares a los de los virus en las funciones de los programas, tales como modificaciones de archivos encubiertas, llamadas en segundo plano de clientes de correo electrónico y otros métodos que los virus pueden utilizar para reproducirse. Cuando el número de estos tipos de comportamientos, o su calidad inherente, alcanza un umbral de tolerancia predeterminado, el motor señala el programa como posible virus.

El motor también "triangula" su evaluación buscando comportamientos del programa que ningún virus mostraría, por ejemplo, la petición al usuario de algún tipo de entrada, a fin de eliminar detecciones positivas falsas. Esta combinación de heurística doble de técnicas "positivas" y "negativas" consigue una velocidad de detección insuperable sin que apenas se produzcan costosas identificaciones erróneas.

Cobertura de amplio espectro

A medida que los agentes dañinos han evolucionado para beneficiarse de la comunicación instantánea y del uso generalizado de Internet, también ha evolucionado el software de VirusScan para hacer frente a las amenazas que presentan. En otro tiempo, un "virus" informático significaba un tipo específico de agente diseñado para reproducirse por sí mismo y ocasionar un daño limitado en el equipo del desafortunado destinatario. Sin embargo, en los últimos años ha surgido un asombroso número de agentes malintencionados que atacan a los usuarios de equipos personales prácticamente desde cualquier ángulo imaginable. Muchos de estos agentes (por ejemplo, algunos de los gusanos que se propagan con mayor rapidez) utilizan versiones actualizadas de antiguas técnicas para infectar los sistemas, pero muchos otros se aprovechan de las nuevas oportunidades que ofrecen las aplicaciones y secuencias de comandos basadas en Web.

Otros incluso abren "puertas traseras" en los sistemas personales o crean "agujeros de seguridad" de una forma que se asemeja más a un intento deliberado de penetrar en la red que a los daños de carácter más aleatorio que la mayoría de los virus dejan a su paso.

Por consiguiente, las últimas versiones del software de VirusScan no esperan a que aparezcan los virus en su sistema, sino que pueden explorar de forma preventiva en el origen o trabajar para impedir que los agentes hostiles lleguen a dicho sistema. El explorador VShield que se incluye con el software de VirusScan tiene tres módulos que se concentran en agentes que llegan de Internet, se propagan a través del correo electrónico o se ocultan en sitios de Internet. Puede buscar objetos Java y ActiveX concretos que supongan una amenaza o bloquear el acceso a sitios de Internet peligrosos. Por otra parte, una extensión del módulo de exploración de correo electrónico para clientes que utilizan este servicio de Microsoft Exchange, por ejemplo Microsoft Outlook, puede hacer una "radiografía" del buzón del servidor para buscar agentes dañinos antes de que lleguen a su equipo.

El software de VirusScan también se autoprotege contra cualquier intento de utilizar sus funciones para dañar su equipo. Algunos creadores de virus incrustan éstos dentro de documentos que, a su vez, los incrustan en otros archivos para intentar impedir su detección. Otros llevan esta técnica hasta el absurdo extremo de construir archivos de almacenamiento comprimidos, muy grandes y recursivos, con la intención de bloquear el explorador cuando busque infecciones. El software de VirusScan explora con precisión la mayoría de los formatos más comunes de archivos comprimidos y de almacenamiento, pero también incluye mecanismos que impiden que se vea atrapado en una búsqueda interminable de virus.

¿Qué incluye el software de VirusScan?

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

- **VirusScan Central.** Es el principal punto de acceso para la utilización de todos los componentes disponibles de McAfee VirusScan. Esta pantalla inicial (vea la figura 1-1) proporciona información como, por ejemplo, la última vez que se llevó a cabo una exploración en busca de virus en el ordenador, los parámetros de VShield que están activados o desactivados, la información DAT disponible y su fecha de creación.

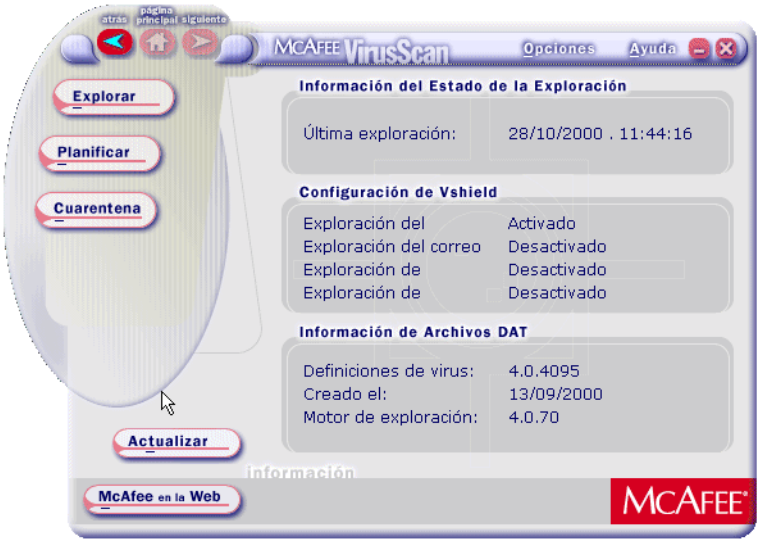

Figura 1-1. Pantalla McAfee VirusScan Central

Mediante esta interfaz de fácil uso puede acceder a las principales funciones de McAfee VirusScan. Haga clic en los botones correspondientes para iniciar una tarea concreta dentro de McAfee VirusScan (por ejemplo, explorar, planificar, poner en cuarentena, etc.).

Asimismo puede hacer clic en el botón Actualizar para iniciar la búsqueda y descarga de las actualizaciones disponibles para el programa McAfee VirusScan instalado en el ordenador. Compruebe que dispone de conexión a Internet antes de utilizar esta función. Para obtener más información, así como instrucciones detalladas, haga clic en el icono de ayuda situado en la esquina superior derecha de la ventana. Para ver las opciones de que dispone para personalizar los componentes de McAfee VirusScan en el ordenador, haga clic en el botón Opciones.

- **La Consola de VirusScan**. Este componente permite crear, configurar y ejecutar tareas de VirusScan a las horas que especifique. Una "tarea" puede incluir desde una operación de exploración de un conjunto de disquetes en un momento o intervalo determinado, hasta una operación de actualización u obtención de una nueva versión del producto. También puede activar o desactivar el explorador VShield desde la ventana Consola.

  La consola incluye una lista predeterminada de tareas que garantizan un nivel mínimo de protección del sistema. Por ejemplo, puede explorar y limpiar el disco C: o todos los discos del ordenador.

- **El explorador VShield**. Este componente proporciona protección constante contra virus que llegan en disquetes, de la red o de varias fuentes de Internet. El explorador VShield se inicia cuando arranca su ordenador y permanece residente en memoria hasta que lo apaga. El flexible conjunto de páginas de propiedades permite indicar al explorador qué partes del sistema se van a explorar, cuáles se van a excluir, qué se debe buscar y el tratamiento que hay que dar a los archivos infectados. Asimismo, el explorador puede avisarle cada vez que encuentre un virus y resumir todas sus acciones.

  El explorador VShield incluye tres módulos especializados adicionales que protegen contra subprogramas Java y controles ActiveX hostiles, exploran mensajes y archivos adjuntos de correo electrónico que se reciben de Internet a través de Lotus cc:Mail, Microsoft Mail o de otros clientes de correo electrónico que cumplan con el estándar MAPI (Interfaz de programación de aplicaciones de mensajería) de Microsoft, y bloquean el acceso a sitios de Internet peligrosos. La protección de la configuración mediante contraseña evita la introducción de modificaciones no autorizadas. Un mismo cuadro de diálogo controla las opciones de configuración de todos los módulos de VShield. Consulte "Utilización del explorador VShield" en la página 91 de la *Guía del usuario* de VirusScan para obtener información detallada.

- **Safe & Sound**. Con este componente puede crear conjuntos de copias de seguridad en archivos de volumen protegidos, que es el tipo mejor y más seguro de copia de seguridad. Un *archivo de volumen protegido* es un área independiente de la unidad, denominada algunas veces unidad lógica.

NOTA: Safe & Sound sólo está disponible para Windows 95, 98 y Windows ME. Para más información, consulte el capítulo 9 "Acerca de Safe & Sound".

- **Cuarentena**. Con este componente puede desplazar los archivos infectados a una carpeta de cuarentena. De esta forma, los retira de las zonas en las que pueden abrirse y puede limpiarlos o borrarlos a su conveniencia.

NOTA: Para más información, consulte el capítulo 10 "Acerca de Cuarentena".

- **La extensión Exploración de correo electrónico**. Este componente permite explorar el buzón en Microsoft Exchange u Outlook, o las carpetas públicas a las que tenga acceso, directamente en el servidor. Esta valiosa "radiografía" del buzón significa que el software de VirusScan puede detectar infecciones potenciales antes de que lleguen a su equipo, lo cual permite evitar virus del tipo Melissa.
- **Un explorador cc:Mail**. Este componente incluye tecnología optimizada para la exploración de los buzones de Lotus cc:Mail que no utilizan el estándar MAPI. Instale y utilice este componente si la red o grupo de trabajo utiliza la versión 8.x de cc:Mail o una anterior.
- **La utilidad de configuración de cliente del Administrador de alertas**. Este componente permite seleccionar un destino para los "sucesos" del Administrador de alertas que el software de VirusScan genera cuando detecta un virus o realiza otras acciones a tener en cuenta. También puede especificar un directorio de destino para mensajes más antiguos de Alertas centralizadas o complementar ambos métodos con alertas DMI (Interfaz de administración del equipo) enviadas a través del software cliente DMI.
- **La utilidad ScreenScan**. Este componente opcional explora el ordenador cuando se activa el protector de pantalla en períodos de inactividad.
- **La utilidad SendVirus**. Este componente proporciona un método fácil para someter los archivos que considere infectados directamente al examen de los exploradores antivirus de McAfee VirusScan. Un sencillo asistente le guiará para seleccionar los archivos que se van a explorar, incluir información de contacto y, si lo prefiere, eliminar datos personales o confidenciales de los archivos de documentos.
- **La utilidad de creación de discos de emergencia**. Esta utilidad esencial le ayuda a crear un disquete que puede utilizar para iniciar el equipo en un entorno sin virus y después explorar las zonas más importantes del sistema para eliminar cualquier virus que pueda cargarse al arrancar.

- **Exploradores de línea de comandos**. Este componente consta de un conjunto de exploradores con todas las funciones que puede utilizar para ejecutar operaciones de exploración concretas desde las ventanas de símbolo de MS-DOS, interfaz de comandos o símbolo del sistema, o desde el modo protegido MS-DOS. El conjunto incluye lo siguiente:

  – FINDVIRU.EXE, un explorador sólo para entornos de 32 bits. Es la interfaz principal de línea de comandos. Cuando se ejecuta este archivo, primero comprueba si su entorno le permite ejecutarse por sí mismo. Si el equipo funciona en un entorno de 16 bits o en modo protegido, transfiere el control a otro de los exploradores.

  – SCANPM.EXE, un explorador para entornos de 16 y 32 bits. Este explorador proporciona un conjunto completo de opciones de exploración para entornos de DOS en modo protegido de 16 y 32 bits. También admite asignaciones de memoria extendida y memoria flexible. FINDVIRU.EXE transfiere el control a este explorador si sus funciones permiten que la operación de exploración se realice más eficazmente.

  – SCAN86.EXE, un explorador sólo para entornos de 16 bits. Este explorador incluye un conjunto limitado de opciones dirigidas a entornos de 16 bits. FINDVIRU.EXE transfiere el control a este explorador si su equipo funciona en modo de 16 bits, pero sin configuraciones de memoria especiales.

  – BOOTSCAN.EXE, un explorador especializado, más pequeño, que se utiliza principalmente con la utilidad de creación de discos de emergencia. Este explorador se ejecuta normalmente desde un disquete creado para obtener un entorno de arranque sin virus.

    Cuando se ejecuta el asistente para creación de discos de emergencia, el software de VirusScan copia BOOTSCAN.EXE y un conjunto especializado de archivos .DAT en un solo disquete. BOOTSCAN.EXE no detectará ni limpiará virus de macros, pero sí que lo hará con otros virus que puedan poner en peligro la instalación del software de VirusScan o infectar archivos al iniciar el sistema. Una vez que identifica y da respuesta a esos virus, puede ejecutar sin peligro el software de VirusScan para limpiar el resto del sistema.

Todos los exploradores de línea de comandos permiten iniciar operaciones de exploración concretas desde las ventanas del símbolo del sistema o de MS-DOS, o desde el modo protegido MS-DOS. Normalmente, utilizará la interfaz gráfica de usuario (GUI) de la aplicación VirusScan para 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 línea de comandos como copias de seguridad.

- **Documentación.** La documentación del software de VirusScan incluye:

  – Una *Guía de inicio rápido* impresa en la que se presenta el producto, se detallan las instrucciones para su instalación, se describe el modo de proceder si se sospecha que el equipo está infectado con un virus y se proporciona una descripción general del producto. La *Guía de inicio rápido* impresa se incluye con las copias del software de VirusScan distribuidas en CD-ROM y también puede descargarse como archivo vs51_getstart. PDF del sitio Web de Network Associates o de otros servicios electrónicos.

  – Esta guía del usuario se guarda en el CD-ROM del software de VirusScan o se instala en el disco duro en formato .PDF de Adobe Acrobat. También puede copiarla como archivo vscan51_userguide.PDF del sitio Web de Network Associates o de otros servicios electrónicos. En la *Guía del usuario de VirusScan* se describe en detalle la utilización del programa y se proporciona información útil sobre, por ejemplo, las opciones de configuración avanzada y de funcionamiento en segundo plano. Los archivos .PDF de Acrobat son documentos en línea flexibles que contienen hipervínculos, resúmenes y otras ayudas que facilitan la navegación y la extracción de información.

  – Una guía del administrador, que se guarda en el CD-ROM del software de VirusScan o se instala en el disco duro en formato .PDF de Adobe Acrobat. La *Guía del administrador de VirusScan* describe en detalle cómo administrar y configurar el software de VirusScan desde un equipo local o remoto.

  – Un archivo de ayuda en línea. Este archivo proporciona acceso rápido a un conjunto completo de temas que describen el software de VirusScan. Puede abrir este archivo seleccionando **Temas de Ayuda** en el menú **Ayuda** de la ventana principal de VirusScan o haciendo clic en cualquiera de los botones de **Ayuda** que aparecen en los cuadros de diálogo de VirusScan.

El archivo de ayuda también incluye amplia ayuda contextual o ayuda "¿Qué es esto?". Para mostrar estos temas de ayuda, haga clic con el botón derecho del ratón en los botones, listas, iconos, algunos cuadros de texto y otros elementos que vea en los cuadros de diálogo. También puede hacer clic en el signo **?** que aparece en la parte superior derecha de la mayoría de los cuadros de diálogo y después hacer clic en el elemento cuya descripción desea ver para mostrar el tema correspondiente. Los cuadros de diálogo con botones de **Ayuda** abren el archivo de ayuda en el tema específico que describe todo el cuadro de diálogo.

- Archivo LICENCIA.TXT. Este archivo incluye los términos de la licencia del software de VirusScan. Léalo atentamente, ya que la instalación del software de VirusScan supone su aceptación.
- Archivo LEAME.TXT. Este archivo contiene cambios o adiciones de última hora respecto a la documentación, enumera los comportamientos conocidos u otros aspectos relacionados con la versión del programa, y a menudo describe nuevas funciones incorporadas en las actualizaciones más recientes. Puede encontrar el archivo LEAME.TXT en el directorio raíz del CD-ROM del software de VirusScan o en la carpeta de programa del software de VirusScan y abrirlo e imprimirlo desde el Bloc de notas de Windows o prácticamente desde cualquier software de procesamiento de textos.

Novedades de esta versión

Esta versión de VirusScan introduce una serie de funciones innovadoras en la funcionalidad básica del producto, en su ámbito de cobertura y en los detalles de la arquitectura de la aplicación. No obstante, el cambio más significativo con respecto a versiones anteriores de VirusScan es la integración de dos versiones independientes de VirusScan, optimizadas para funcionar en plataformas distintas de Windows, en un sólo producto que funciona en las dos versiones. Este único producto aprovecha las ventajas específicas de cada plataforma.

Las secciones siguientes describen otros cambios que introduce esta versión de VirusScan.

Funciones de instalación y distribución

Los productos antivirus de McAfee VirusScan, incluido el software de VirusScan, utilizan ahora MSI (Instalador de Microsoft Windows), que se incluye con todos los sistemas Windows 2000 Professional. Esta utilidad de instalación ofrece numerosas funciones personalizadas de instalación y configuración que permiten distribuir el software de VirusScan de manera más fácil e intuitiva.

Mejoras de la interfaz

Esta versión introduce de forma sólida la interfaz de VirusScan para todas las plataformas admitidas en el territorio en que el software antivirus de VirusScan para Windows 95, Windows 98 y Windows ME fue pionero con su versión 4.0.1. Con ello se añaden numerosas opciones de configuración del explorador VShield para las plataformas Windows NT Workstation versión 4.0 y Windows 2000 Professional, reduciéndose la complejidad anterior de algunas de estas opciones. Por ejemplo, la configuración del servidor del Administrador de alertas pasa en su totalidad a la línea de productos NetShield; el software de VirusScan funciona ahora estrictamente como aplicación cliente configurable.

Esta versión también proporciona un nuevo panel de control de VirusScan, que funciona como punto central desde el que se pueden activar y desactivar todos los componentes de VirusScan. Este panel de control permite definir además el número máximo de elementos que se pueden explorar o excluir en una sola operación, así como determinar que se ejecuten el explorador VShield y el panel de control de VirusScan al iniciar el sistema. Otros cambios que se incluyen son los siguientes:

- Nuevos estados en el icono de la bandeja del sistema Vshield, que proporcionan más información sobre qué módulos de VShield están activos. Estos estados son los siguientes:
  -  Todos los módulos de VShield están activos
  -  El módulo Exploración de sistema está activo, pero uno o varios de los demás módulos de VShield están inactivos
  -  El módulo Exploración de sistema está inactivo, pero uno o varios de los demás módulos de VShield están activos
  -  Todos los módulos de VShield están inactivos
- Nuevas opciones de interfaz para configuración de tareas que permiten indicar a la aplicación VirusScan cómo debe aparecer al ejecutar la tarea programada y qué debe hacer cuando termine. También puede definir una contraseña para impedir que se realicen cambios en la configuración de tareas individuales o para proteger la configuración de toda la tarea.
- Una función aleatoria actualizada para tareas programadas permite definir una hora de ejecución de la tarea y, a continuación, una "ventana" aleatoria. Después la Consola de VirusScan elige una hora aleatoria en la ventana para iniciar realmente la tarea.
- Las opciones de acción del módulo Exploración de sistema incluyen ahora una nueva opción de configuración Tipo de comando para los sistemas Windows 95 y Windows 98. Esta opción permite determinar cómo aparecerá la alerta **Consultar al usuario antes de realizar acción**.

Cambios en la funcionalidad del producto

- Una nueva utilidad de configuración del cliente del Administrador de alertas permite elegir un servidor del Administrador de alertas instalado en la red como destino de los mensajes de alerta, o seleccionar una red compartida como destino de mensajes de Alertas centralizadas. También puede complementar cualquiera de estos dos métodos de alerta con mensajes de alerta de la interfaz de administración del equipo.
- El servidor del Administrador de alertas admite los números de serie del procesador Intel Pentium III para identificar equipos individuales en la notificación de virus. Para obtener más información acerca de los números de serie del procesador Intel, consulte la lista de preguntas más frecuentes de Intel en la dirección http://support.intel.com/support/processors/pentiumiii/psqa.htm.

Nuevas opciones de actualización para el software de VirusScan

Aunque la mayoría de las definiciones de virus que necesita se incorporan ahora directamente a su motor en forma de rutinas genéricas, el software de VirusScan sigue necesitando actualizaciones periódicas de los archivos .DAT para estar al día de los 200 a 300 virus nuevos que aparecen cada mes. Para satisfacer esta necesidad, McAfee VirusScan ha incorporado al software de VirusScan tecnología de actualización procedente de sus primeras fases. Con esta versión, ese tipo de tecnología da un salto espectacular en la actualización de archivos .DAT incrementales.

El servicio SecureCast de Network Associates proporciona un método cómodo para recibir las últimas actualizaciones de archivos (.DAT) de definición de virus de forma automática a medida que estén disponibles y sin tener que descargarlos.

NOTA: Para actualizar el software McAfee VirusScan instalado en el ordenador, haga clic en el botón **actualizar** de la ventana principal de McAfee VirusScan. Compruebe que el PC está conectado a Internet antes de realizar esta tarea.

Instalación del software de VirusScan 2

Antes de comenzar

McAfee VirusScan Software distribuye el software de VirusScan de dos formas: 1) como un archivo de almacenamiento que puede descargar desde el sitio Web de McAfee; y 2) en CD-ROM. Aunque la forma de transferir los archivos de VirusScan desde un archivo de almacenamiento que se descarga difiere del método que se utiliza para transferir los archivos desde un CD-ROM insertado en la unidad de CD-ROM, los pasos de instalación que se deben seguir tras esa fase son los mismos para ambos tipos de distribución. Revise los requisitos del sistema para comprobar que el software VirusScan puede ejecutarse en su sistema.

Requisitos del sistema

El software de VirusScan puede instalarse y ejecutarse en cualquier PC IBM o compatible equipado con:

- Un procesador equivalente al menos a un procesador Intel tipo Pentium o compatible. McAfee VirusScan recomienda un procesador Intel Pentium o Celeron con una velocidad de ejecución mínima de 166 MHz.
- Una unidad de CD-ROM. Si descarga una copia del software de VirusScan, este elemento es opcional.
- Un mínimo de 40 MB de espacio libre en disco para una instalación completa. McAfee VirusScan recomienda 75 MB.
- Un mínimo de 16 MB de memoria de acceso aleatorio (RAM) libre. McAfee VirusScan recomienda un mínimo de 20 MB.
- Microsoft Windows 95, Windows 98, Windows ME, Windows NT Workstation versión 4.0 con Service Pack 4 o posterior, o Windows 2000 Professional. McAfee VirusScan recomienda asimismo tener instalado Microsoft Internet Explorer versión 4.0.1 o posterior, especialmente si el sistema funciona con alguna versión de Windows 95.

Otras recomendaciones

Para obtener el máximo provecho de las características de actualización automática del software de VirusScan debe disponer de conexión a Internet a través de un módem de alta velocidad y un proveedor de servicios de Internet.

Preparación para instalar el software de VirusScan

Tras introducir el disco de McAfee VirusScan en la unidad de CD-ROM, aparece automáticamente una pantalla de bienvenida de VirusScan. Si desea instalar el software de VirusScan inmediatamente, haga clic en **Instalar VirusScan** y vaya al paso 4 para continuar. Si la pantalla de bienvenida no aparece o si va a instalar el software de VirusScan desde archivos descargados, comience en el paso 2.

IMPORTANTE: Puesto que el programa de instalación instala algunos archivos de VirusScan como servicios en los sistemas Windows NT Workstation versión 4.0 y Windows 2000 Professional, debe iniciar la sesión en su sistema con derechos de administrador para poder instalar este producto. Para ejecutar el programa de instalación en Windows 95 o Windows 98, no necesita iniciar la sesión con unos derechos o un perfil específicos.

Opciones de instalación

En la sección dedicada a los pasos para la instalación se describe cómo instalar el software de VirusScan con sus opciones más comunes en un equipo o estación de trabajo individual. Puede optar por realizar una instalación típica, que instala los componentes de uso común de VirusScan pero excluye algunos módulos de VShield y la utilidad ScreenScan, o realizar una instalación personalizada que permite instalar todos los componentes de VirusScan.

Pasos de instalación

McAfee VirusScan recomienda cerrar todas las aplicaciones que se estén ejecutando en el sistema antes de iniciar la instalación. De esta forma se reduce la posibilidad de que algún conflicto de software afecte a la instalación.

Para instalar el software de VirusScan, proceda como se indica a continuación:

1. Si su equipo utiliza Windows NT Workstation versión 4.0 o Windows 2000 Professional, conéctese al sistema como administrador. Para instalar el software de VirusScan en el sistema necesita tener derechos de administración.

2. Seleccione **Ejecutar** en el menú **Inicio** de la barra de tareas de Windows.

   Aparecerá el cuadro de diálogo Ejecutar (Figura 2-1).

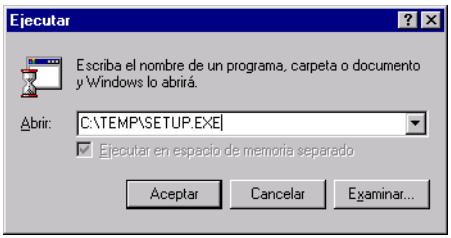

Figura 2-1. Cuadro de diálogo Ejecutar

3. 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 extraídos de VirusScan. Para localizar los archivos correctos en el disco duro o en el CD-ROM, haga clic en **Examinar**.

- **NOTA:** Si la copia del software de VirusScan incluye un CD-ROM de Active Virus Defense o Total Virus Defense, también debe especificar la carpeta que contiene dicho software.

Antes de continuar, el programa de instalación comprueba si el sistema ya tiene la versión 1.1 de la utilidad MSI (Instalador de Microsoft Windows) funcionando como parte del software.

Si el equipo utiliza Windows 2000 Professional, esta versión de MSI ya existe en el sistema. Si su equipo utiliza una versión anterior de Windows, puede que ya disponga de esta versión de MSI si ha instalado con anterioridad otro software que también use MSI. En ambos casos, el programa de instalación mostrará inmediatamente el primer panel del asistente. Continúe en el paso 4.

Si el programa de instalación no encuentra MSI versión 1.1 en el equipo, instalará los archivos que necesite para continuar con la instalación y le solicitará que reinicie el equipo. Haga clic en **Reiniciar sistema**.

Al reiniciar el equipo, el programa de instalación continuará desde el punto en que se detuvo. Aparecerá la pantalla de bienvenida del programa de instalación (Figura 2-2).

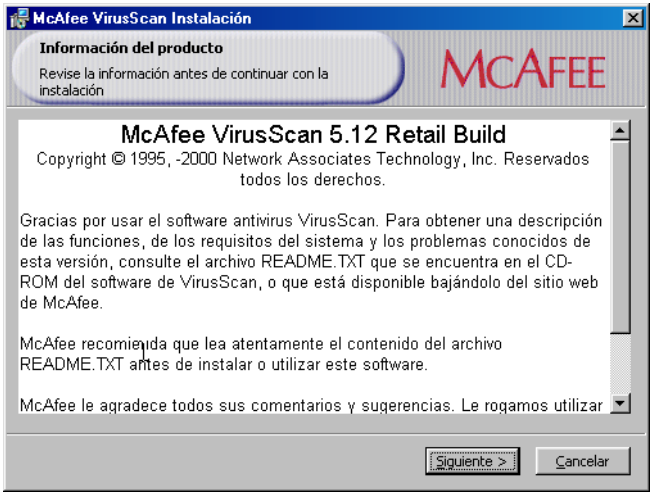

Figura 2-2. Pantalla de bienvenida del programa de instalación

4. Este primer panel indica dónde se encuentra el archivo LEAME.TXT, que describe las funciones del producto, enumera los temas conocidos e incluye la última información del producto disponible sobre esta versión de VirusScan. Cuando haya leído el texto, haga clic en **Siguiente>** para continuar.

5. El siguiente panel del asistente muestra el acuerdo de licencia de usuario final del software de VirusScan. Léalo detenidamente ya que al instalar el software de VirusScan estará aceptando sus términos.

   Si no acepta los términos de la licencia, seleccione **No acepto los términos del acuerdo de licencia** y después haga clic en **Cancelar**. La instalación se anulará inmediatamente. En caso contrario, haga clic en **Acepto los términos del acuerdo de licencia** y después haga clic en **Siguiente>** para continuar.

   Seguidamente el programa de instalación comprueba si existen versiones anteriores de VirusScan o software incompatible en el equipo. Si no tiene otro software antivirus ni versiones anteriores de VirusScan en el sistema, aparecerá el panel de tipo de seguridad o de tipo de instalación. Continúe en el paso 8.

   Si el programa de instalación detecta una versión anterior de VirusScan en el sistema, le indicará que debe eliminarla. Si el equipo utiliza Windows 95 o Windows 98, el programa de instalación también le ofrece la opción de conservar la configuración de VShield que seleccionó para la versión anterior.

Si utiliza Windows NT Workstation v4.0 o Windows 2000 Professional, el programa de instalación eliminará la versión anterior de VirusScan, pero *no* conservará la configuración anterior del explorador VShield.

6. Seleccione la opción **Conservar configuración automática**, si está disponible, y haga clic en **Siguiente>** para continuar.

   Si el programa de instalación detecta software incompatible, mostrará un panel del asistente en el que podrá eliminar el software en conflicto (vea la figura 2-3).

   Si no tiene software incompatible en el sistema y utiliza Windows 95 o Windows 98, vaya al paso 9 para continuar con la instalación. Si no tiene software incompatible y el sistema utiliza Windows NT Workstation versión 4.0 o Windows 2000 Professional, vaya al paso 8 para continuar. En caso contrario, continúe con el paso 7.

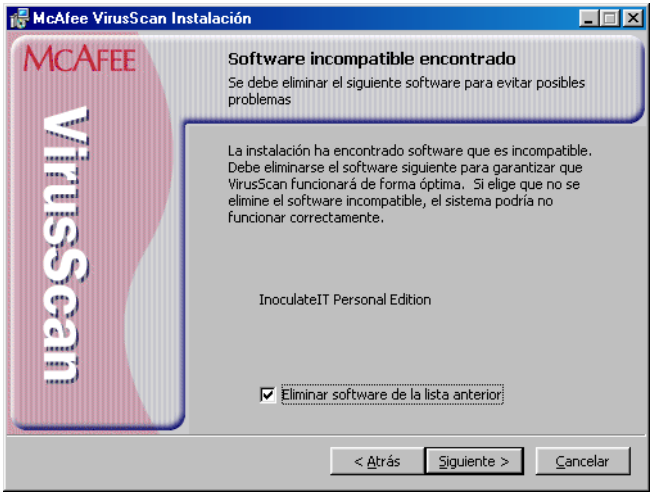

Figura 2-3. Panel de software incompatible

7. Active la casilla de verificación y, a continuación, haga clic en **Siguiente>**. El programa iniciará la utilidad de desinstalación que utiliza normalmente el software que ocasiona el conflicto permitiendo su eliminación. La utilidad de desinstalación puede informarle de que es necesario reiniciar el sistema para eliminar totalmente el otro software. *No* necesita hacerlo para continuar con la instalación de VirusScan; mientras no esté activo el otro software, el programa de instalación puede continuar sin que se produzcan conflictos.

- **NOTA:** McAfee VirusScan recomienda encarecidamente que elimine el software incompatible. Debido a que la mayoría del software antivirus funciona a un nivel muy bajo en el sistema, dos programas antivirus que compitan por acceder a los mismos archivos o que realicen operaciones esenciales pueden ocasionar gran inestabilidad en el sistema.

Si el equipo utiliza Windows NT Workstation versión 4.0 o Windows 2000 Professional, el programa de instalación preguntará qué modo de seguridad desea utilizar para ejecutar el software de VirusScan en el sistema.

Las opciones de este panel determinan si otros usuarios pueden utilizar el equipo para realizar cambios en las opciones de configuración que seleccione, para programar y ejecutar tareas o para activar y desactivar componentes de VirusScan. El software de VirusScan incluye amplias medidas de seguridad que impiden que usuarios no autorizados puedan realizar cambios en las configuraciones de software en el modo de máxima seguridad. El modo de seguridad estándar permite a todos los usuarios tener acceso a todas las opciones de configuración.

Cualquiera de las opciones que seleccione instalará la misma versión de VirusScan, con las mismas opciones de configuración y las mismas tareas programadas para todos los usuarios del sistema.

8. Seleccione el modo de seguridad que prefiera. Podrá elegir entre las siguientes opciones:

   - **Utilizar seguridad máxima**. Seleccione esta opción si desea que sólo los usuarios con derechos de administrador sobre su equipo puedan cambiar opciones de configuración, activar o desactivar componentes de VirusScan o configurar y ejecutar tareas programadas.

     Los usuarios que no tengan derechos de administrador podrán configurar y ejecutar sus operaciones de exploración con la aplicación VirusScan y guardar la configuración de esas operaciones en un archivo .VSC, pero no podrán cambiar la configuración predeterminada de la aplicación VirusScan.

   - **Utilizar seguridad estándar**. Seleccione esta opción si desea que los usuarios que se conecten a su equipo puedan cambiar opciones de configuración, activar o desactivar componentes de VirusScan o programar y ejecutar tareas.

   A continuación, el programa de instalación pide que seleccione una instalación típica o personalizada para el equipo.

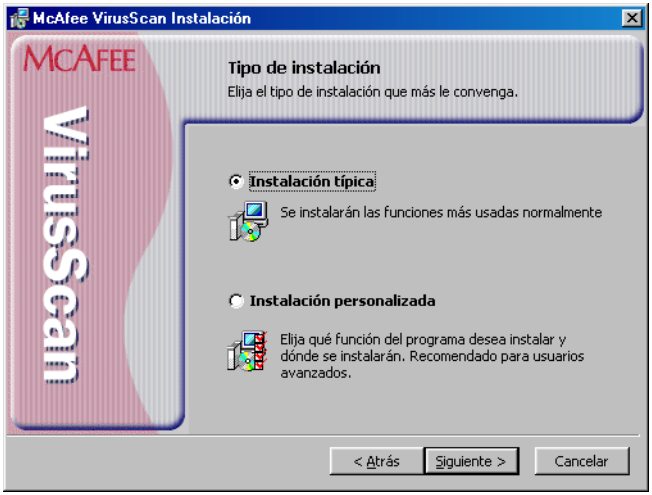

Figura 2-4. Panel de tipo de instalación

9. Seleccione el tipo de instalación que prefiera. Podrá elegir entre las siguientes opciones:

   - **Instalación típica**. Con esta opción se instalan todas las funciones del producto McAfee VirusScan.
   - **Instalación personalizada**. Con esta opción puede personalizar McAfee VirusScan seleccionando funciones concretas para su instalación en el ordenador.

10. Seleccione la opción que prefiera y haga clic en **Siguiente>** para continuar.

    Si selecciona **Instalación personalizada**, aparecerá el panel que se muestra en la figura 2-5. En caso contrario, siga en el paso 13 para continuar la instalación.

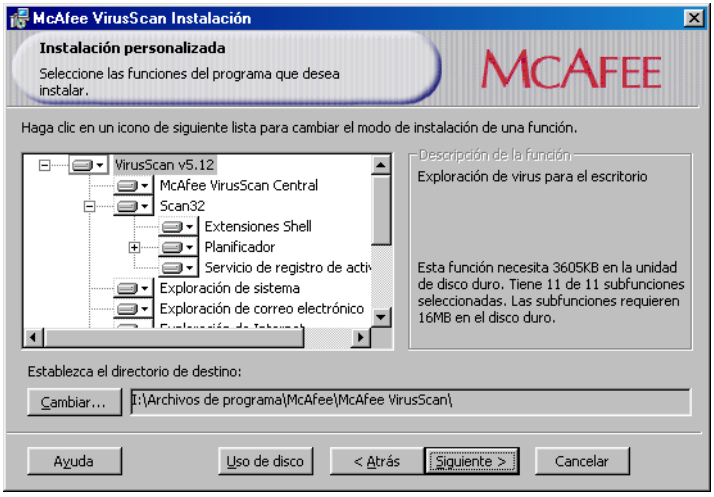

Figura 2-5. Panel de instalación personalizada

11. Seleccione los componentes de VirusScan que desee instalar. Podrá:

    - Agregar un componente a la instalación. Haga clic junto al nombre de un componente y después seleccione **Esta función se instalará en la unidad de disco duro local** en el menú que aparece. Para agregar un componente y cualquier módulo relacionado del componente, seleccione **Esta función y todas las funciones secundarias se instalarán en la unidad de disco duro local**. Sólo puede seleccionar esta opción si un componente tiene módulos relacionados.

    - Eliminar un componente de la instalación. Haga clic en junto al nombre de un componente y, a continuación, seleccione **Esta función no estará disponible** en el menú que aparece.

    - **NOTA:** La utilidad de instalación de VirusScan no admite las demás opciones que se muestran en este menú. No se pueden instalar los componentes de VirusScan para ejecutarlos desde una red, y el software de VirusScan no tiene componentes que se puedan instalar según sean necesarios.

También puede especificar un disco y un directorio de destino diferentes para la instalación. Haga clic en **Cambiar** y localice la unidad o el directorio que desee utilizar en el cuadro de diálogo que aparece. Para ver un resumen de las necesidades de disco de VirusScan con respecto al espacio disponible en el disco, haga clic en **Uso del disco**. El asistente resaltará los discos que tengan espacio insuficiente.

12. Cuando haya seleccionado los componentes que desee instalar, haga clic en **Siguiente>** para continuar.

    El programa de instalación mostrará un panel del asistente confirmando que está preparado para comenzar a instalar archivos (Figura 2-6).

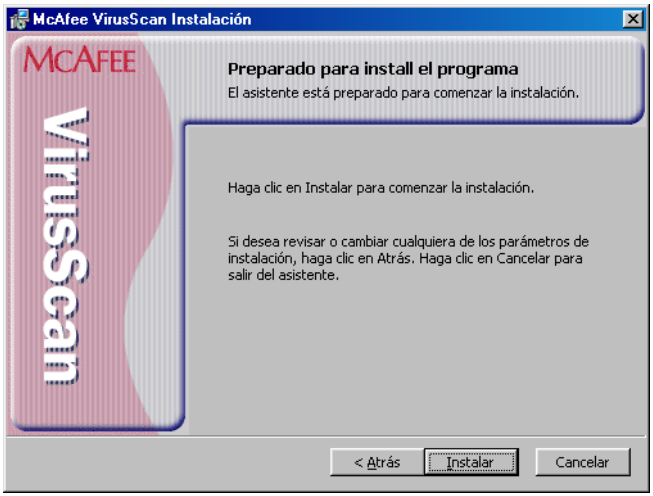

Figura 2-6. Panel de asistente preparado para instalar

13. Haga clic en **Instalar** para comenzar a copiar archivos en la unidad de disco duro. De lo contrario, haga clic en **<Atrás** para cambiar las opciones de instalación que haya seleccionado.

    El programa de instalación elimina del sistema las versiones del software de VirusScan anteriores o incompatibles y después copia los archivos de programa de VirusScan en el disco duro. Cuando haya terminado, muestra un panel que pregunta si desea configurar el producto que ha instalado (Figura 2-7).

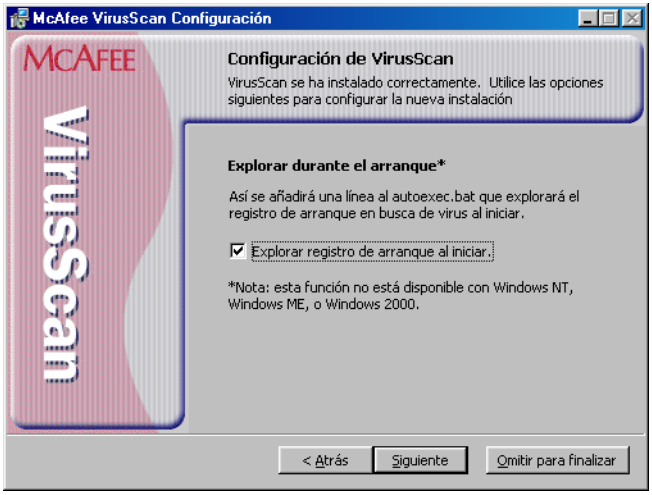

Figura 2-7. Panel de configuración de VirusScan

14. Desde el panel de configuración de VirusScan (figura 2-7), puede hacer caso omiso de la configuración para finalizar la instalación u optar por configurar las opciones disponibles que aparecen en pantalla.

    - **Explorar registro de arranque al inicio**. Active esta casilla de verificación para que el programa de instalación escriba estas líneas en el archivo AUTOEXEC.BAT de Windows:

      C:\PROGRA~1\COMMON~1\NETWOR~1\VIRUSS~1\40~1.XX\SCAN
      .EXE C:\
      @IF ERRORLEVEL 1 PAUSE

      Indican al sistema que inicie el explorador del programa de línea de comandos de VirusScan al arrancar. El explorador, a su vez, se detendrá si detecta un virus en el sistema para que pueda salir y utilizar el disco de emergencia de VirusScan para reiniciar.

      Si el equipo utiliza Windows NT Workstation versión 4.0, Windows ME o Windows 2000 Professional, no podrá seleccionar **Explorar registro de arranque al inicio**, pero podrá elegir cualquiera de las otras opciones. Ni Windows NT Workstation, Windows ME, ni Windows 2000 permiten que el software explore o realice cambios en sectores de arranque del disco o en registros de arranque maestros. Además, estos sistemas operativos no utilizan un archivo AUTOEXEC.BAT para iniciar el sistema.

15. En el siguiente grupo de pantallas aparecerán opciones para ejecutar otros componentes de McAfee VirusScan como, por ejemplo, la utilidad Safe & Sound, la actualización de VirusScan y la utilidad de disco de rescate (figura 2-8).

NOTA: La utilidad Safe & Sound no puede utilizarse con Windows NT ni Windows 2000.

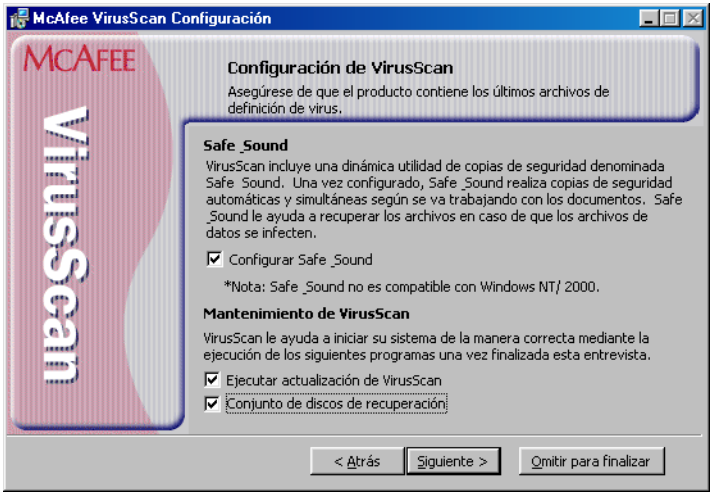

Figura 2-8. Panel de configuración

Seleccionar las opciones de configuración correspondientes a su instalación. Puede optar por explorar el sistema, crear un disco de emergencia o actualizar los archivos de definición de virus antes de iniciar el explorador VShield y la Consola de VirusScan.

NOTA: Para más información sobre cualquiera de estas opciones, puede consultar la ayuda en línea de McAfee VirusScan.

16. En la siguiente pantalla (figura 2-9), active la casilla de verificación de **Activación de la protección McAfee VirusScan** y haga clic en **Finalizar**. Aparecerán las "pantallas de presentación" del software de VirusScan, y en la bandeja del sistema de Windows se mostrarán los iconos del explorador VShield y de la Consola de VirusScan. El software está preparado para su utilización.

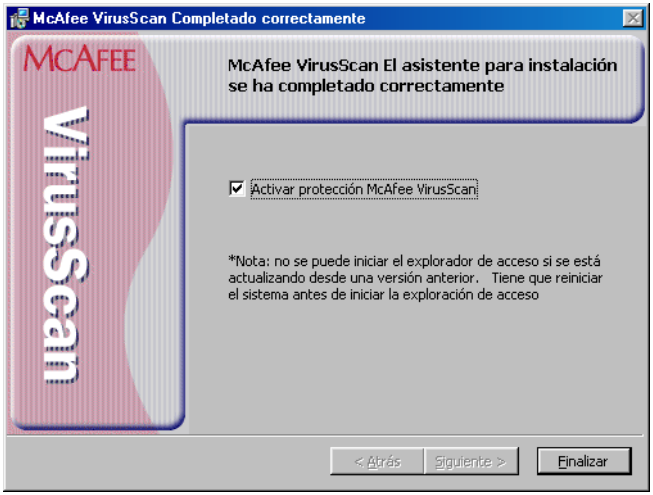

Figura 2-9. Panel de instalación correcta

17. Tras hacer clic en Finalizar, aparece el cuadro de diálogo de información del instalador de McAfee VirusScan en el que se le indicará que reinicie el ordenador (figura 2-10).

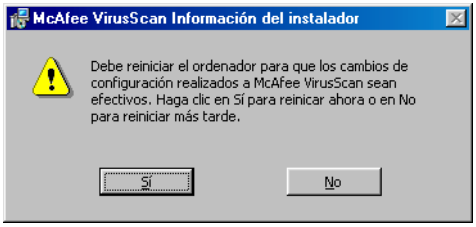

Figura 2-10. Cuadro de diálogo de información del instalador de McAfee VirusScan

- **NOTA:** Si tenía una versión anterior de VirusScan instalada en el equipo, tendrá que reiniciar el sistema para poder iniciar el explorador VShield. Haga clic en Sí para reiniciar el ordenador.

Uso de la utilidad para creación del disco de emergencia

Si decide crear un disco de emergencia durante la instalación, el programa interrumpe la instalación del software de VirusScan, inicia el asistente para creación del disco de emergencia y, cuando termina, vuelve a la secuencia de instalación. Para obtener información sobre la creación de un disco de emergencia, empiece en el paso 1. También puede iniciar el asistente para creación de disco de emergencia en cualquier punto una vez instalado el software VirusScan.

- **NOTA:** McAfee VirusScan recomienda crear el disco de emergencia durante la instalación, después de que el software de VirusScan haya explorado la memoria del sistema en busca de virus. Si el software de VirusScan detecta un virus en el sistema, *no* cree el disco de emergencia en el equipo infectado.

El disco de emergencia creado incluye BOOTSCAN.EXE, un explorador de línea de comandos especializado en pequeñas huellas que puede explorar los sectores de arranque y el Registro de arranque principal (MBR) del disco duro. BOOTSCAN.EXE funciona con un conjunto especializado de archivos .DAT que se centra en eliminar los virus en los sectores de arranque. Si ya tiene instalado el software de VirusScan con las opciones de instalación predeterminadas, puede encontrar estos archivos .DAT en la siguiente ubicación del disco duro:

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

Los archivos .DAT especiales son los siguientes:

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

McAfee VirusScan actualiza periódicamente estos archivos .DAT para detectar nuevos virus en los sectores de arranque. Puede descargar archivos .DAT de emergencia actualizados de la siguiente ubicación:

http://www.nai.com/asp_set/anti_virus/avert/tools.asp

- **NOTA:** McAfee VirusScan recomienda descargar los nuevos archivos .DAT de emergencia directamente en el disquete recién formateado a fin de reducir el riesgo de infección.

Debido a que el asistente cambia el nombre de los archivos y los prepara para utilizarlos al crear el disquete, no puede copiarlos directamente en un disco de emergencia que haya creado personalmente. Utilice el asistente para creación del disco de emergencia para prepararlo.

Para iniciar el asistente después de la instalación, haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Programas** y después **McAfee VirusScan**. A continuación, elija **Crear disco de emergencia**.

Aparecerá el panel de bienvenida del asistente para creación del disco de emergencia (Figura 2-11).

Figura 2-11. Panel de bienvenida del asistente para creación del disco de emergencia

1. Haga clic en **Siguiente>** para continuar.

   Aparece el siguiente panel del asistente (Figura 2-12).

Figura 2-12. Segundo panel del asistente para creación del disco de emergencia

Si el equipo utiliza Windows NT Workstation o Windows 2000 Professional, el asistente indicará que va a formatear el disco de emergencia con NAI-OS.

Debe utilizar estos archivos del sistema operativo patentado para crear el disco de emergencia, porque los de los sistemas Windows NT Workstation v4.0 y Windows 2000 Professional no caben en un solo disquete.

Si el equipo utiliza Windows 95 o Windows 98, el asistente ofrecerá formatear el disco de emergencia con NAI-OS o con archivos de inicio de Windows.

2. Si el asistente permite elegir, indique el sistema operativo cuyos archivos desea utilizar y después haga clic en **Siguiente>** para continuar. Dependiendo del sistema operativo que seleccione, el asistente muestra a continuación un panel diferente:

   - Si ha optado por formatear el disco con NAI-OS, el asistente muestra un panel informativo.

     Para continuar, siga estos pasos:

     a. Inserte un disquete de 1,4 MB que no esté protegido contra escritura y sin formatear, en la unidad de disquete y, a continuación, haga clic en **Siguiente>**.

        El asistente para creación del disco de emergencia copiará sus archivos desde una imagen de disco almacenada en el directorio de programa de VirusScan. Mientras lo hace, mostrará su progreso en un panel del asistente.

     b. Haga clic en **Finalizar** para salir del asistente una vez creado el disco.

     A continuación, extraiga el disquete de la unidad, protéjalo contra escritura, póngale la etiqueta *Disco de arranque de emergencia de McAfee* y guárdelo en un lugar seguro.

   - Si eligió formatear el disco con archivos del sistema de Windows, el asistente mostrará un panel que permite elegir si desea formatear el disquete.

     Podrá elegir entre las siguientes opciones:

   - Si tiene un disquete *sin virus* formateado que sólo contiene archivos de sistema DOS o Windows, insértelo en la unidad de disquete. A continuación, active la casilla de verificación **No formatear** y haga clic en **Siguiente>** para continuar.

Esto indica al asistente para creación del disco de emergencia que copie en el disquete sólo el componente de línea de comandos del software de VirusScan, los archivos .DAT de emergencia y los archivos auxiliares. Continúe en el paso 3.

- Si *no* dispone de un disquete formateado sin virus con archivos de sistema de DOS o Windows, deberá crear uno para utilizar el disco de emergencia e iniciar el equipo. Siga los siguientes pasos:

  a. Inserte un disquete sin formato y sin proteger en la unidad de disquete. McAfee VirusScan recomienda utilizar un disquete totalmente nuevo, que no haya sido formateado con anterioridad, a fin de evitar la posibilidad de infecciones de virus en el disco de emergencia.

  b. Compruebe que la casilla de verificación **No formatear** está desactivada.

  c. Haga clic en **Siguiente>**.

     Aparece el cuadro de diálogo de Windows para formatear disquetes (vea la figura 2-13).

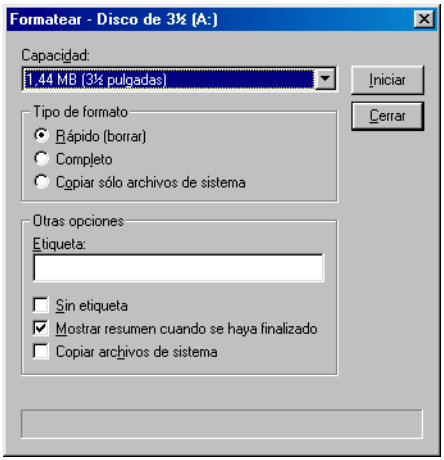

Figura 2-13. Cuadro de diálogo de formato de Windows

  d. Compruebe que la casilla de verificación **Total** del área Tipo de formato y la casilla **Copiar archivos de sistema** del área Otras opciones están seleccionadas. A continuación, haga clic en **Iniciar**.

     Windows formateará el disquete y copiará los archivos de sistema necesarios para iniciar el ordenador.

e. Haga clic en **Cerrar** cuando Windows haya terminado de formatear el disquete y vuelva a hacer clic en **Cerrar** para volver al panel del disco de emergencia.

3. Haga clic en **Siguiente>** para continuar. La utilidad de instalación comprobará si el disquete al que se acaba de dar formato tiene virus (Figura 2-14).

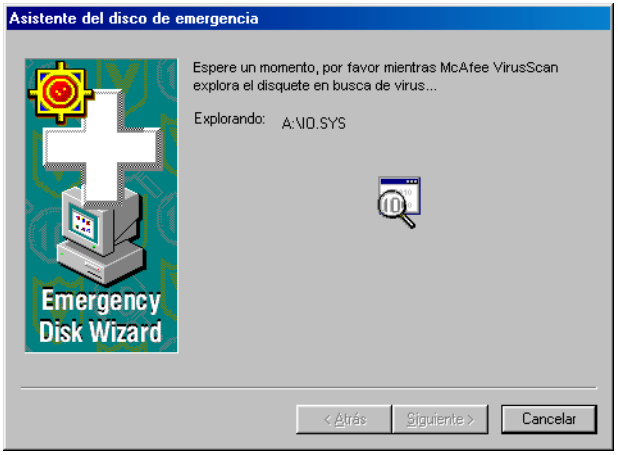

Figura 2-14. Búsqueda de virus en el disco de emergencia

Si el software de VirusScan no detecta ningún virus durante la operación de exploración, la utilidad de instalación copiará inmediatamente BOOTSCAN.EXE y sus archivos auxiliares en el disquete recién creado. Si el software VirusScan *detecta* algún virus, salga inmediatamente de la utilidad de instalación.

4. Cuando el asistente termine de copiar los archivos del disco de emergencia, mostrará el último panel (Figura 2-15).

Figura 2-15. Último panel del asistente para creación del disco de emergencia

5. Haga clic en **Finalizar** para cerrar el asistente. Seguidamente, saque el nuevo disco de emergencia de la unidad de disquetes, póngale una etiqueta, protéjalo contra escritura y guárdelo en un lugar seguro.

- **NOTA**: El disquete estará bloqueado o protegido contra escritura si los dos orificios situados en los extremos del lado opuesto al de la placa deslizante de metal se encuentran abiertos. Si no es así, deslice la pestaña de plástico hasta que los orificios estén totalmente abiertos.

Determinación del momento de reiniciar el equipo

En muchos casos, podrá instalar y utilizar inmediatamente esta versión de VirusScan, sin necesidad de reiniciar el equipo. No obstante, en algunos casos, el instalador de Microsoft Windows (MSI) necesitará reemplazar o inicializar determinados archivos, o puede que el usuario necesite eliminar archivos de instalaciones anteriores del producto McAfee VirusScan para que el software de VirusScan funcione correctamente. Estos requisitos también pueden variar de una plataforma de Windows a otra.

En estos casos tendrá que reiniciar el sistema durante la instalación, generalmente para instalar archivos del instalador de Microsoft (MSI), o después de la misma.

Tabla 2-1. Circunstancias en las que es necesario reiniciar el sistema

Circunstancia	Windows 95 y Windows 98	Windows NT y Windows 2000
Instalación en un equipo sin versión anterior de VirusScan y sin software incompatible	No es necesario reiniciar, a no ser que tenga instalado Novell Client32 para NetWare, en cuyo caso sí es necesario	Es necesario reiniciar
Instalación en un equipo con versión anterior de VirusScan	Es necesario reiniciar	Es necesario reiniciar
Instalación en un equipo con software incompatible	No es necesario reiniciar, pero el programa de instalación preguntará si desea hacerlo. Puede hacer clic con seguridad en **No**.	No es necesario reiniciar, pero el programa de instalación preguntará si desea hacerlo. Puede hacer clic con seguridad en **No**.
Instalación en un equipo con el instalador de Microsoft (MSI) versión 1.0 **NOTA**: Microsoft Office 2000 instala esta versión de MSI	Es necesario reiniciar después de instalar los archivos MSI para que el programa de instalación pueda continuar	Es necesario reiniciar después de instalar los archivos MSI para que el programa de instalación pueda continuar
Instalación en un equipo con el instalador de Microsoft (MSI) versión 1.1	No es necesario reiniciar, salvo en los sistemas con Windows 98 Second Edition o si se utilizan determinados controladores o archivos .DLL	No es necesario reiniciar
Actualización de archivos .DAT	No es necesario reiniciar	No es necesario reiniciar
Actualización del motor de exploración mediante la utilidad SuperDAT de McAfee VirusScan	No es necesario reiniciar	No es necesario reiniciar

Comprobación de la instalación

Una vez instalado, el software de VirusScan está preparado para explorar el sistema en busca de archivos infectados. Puede comprobar si el programa se ha instalado correctamente y si funciona como es debido mediante una prueba desarrollada por el instituto europeo de investigación antivirus (EICAR, European Institute of Computer Anti-virus Research), un consorcio de distribuidores de aplicaciones antivirus, que permite a sus clientes comprobar la instalación de cualquier software antivirus.

Para comprobar la instalación, realice los pasos siguientes:

1. Abra un editor de texto estándar de Windows, como puede ser el Bloc de notas, y, a continuación, escriba esta cadena de caracteres en *una línea sin espacios ni retornos de carro*:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRU-
   TEST-FILE!$H+H*
   ```

   - **NOTA:** La línea anterior tiene que aparecer en *una línea* en la ventana del editor de texto, por lo que debe maximizarla y eliminar los retornos de carro que pueda haber. Asimismo, asegúrese de que escribe la letra O, y no el número 0, en la cadena “X5O...” que inicia el mensaje de prueba.

     Si está leyendo este manual directamente en el ordenador, puede copiar la línea del archivo .PDF de Acrobat y pegarla en el Bloc de notas. También puede copiar esta cadena de texto directamente de la sección “Comprobación de la instalación” del archivo LEAME.TXT, que puede encontrar en el directorio de programas de VirusScan. Si copia la línea de cualquiera de estas fuentes, no olvide eliminar los retornos de carro o espacios que pueda contener.

2. Guarde el archivo con el nombre EICAR.COM. Su tamaño debe ser de 69 o 70 bytes.
3. Inicie el software de VirusScan y configúrelo para que explore el directorio que contiene el archivo EICAR.COM. Cuando el software de VirusScan explore este archivo, indicará que ha encontrado el virus EICAR-STANDARD-AV-TEST-FILE.

   E **IMPORTANTE:** Este archivo *no es un virus.* No puede extenderse, infectar otros archivos ni dañar en modo alguno el sistema. Borre el archivo cuando la comprobación de la instalación haya terminado para evitar que los usuarios que desconozcan este proceso se alarmen innecesariamente.

Modificación o eliminación de la instalación de VirusScan

La versión de MSI (el instalador de Microsoft Windows) que utiliza el software de VirusScan también incluye un método estándar para modificar o eliminar la instalación de VirusScan.

Para modificar o eliminar el software de VirusScan, siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.
2. Haga doble clic en **Agregar o quitar programas**.
3. En el cuadro de diálogo Propiedades de Agregar o quitar programas, seleccione **McAfee VirusScan v5.1** en la lista y después haga clic en **Agregar o quitar**.

   El programa de instalación iniciará y mostrará el primer panel del asistente para mantenimiento del programa.

4. Haga clic en **Siguiente>** para continuar.

   El programa de instalación muestra el panel del asistente para mantenimiento del programa. Decida si desea modificar componentes de VirusScan o eliminar el software de VirusScan totalmente del sistema. Podrá elegir entre las siguientes opciones:

   - **Modificar.** Seleccione esta opción para agregar o eliminar componentes individuales de VirusScan. El programa de instalación mostrará el panel del asistente personalizado (vea la figura 2-5). Comience con el paso 11 para seleccionar los componentes que desee agregar o quitar.
   - **Eliminar.** Seleccione esta opción para eliminar el software de VirusScan totalmente del equipo. El programa de instalación le pedirá que confirme que desea eliminar el software del sistema.

     Haga clic en **Quitar**. El programa de instalación mostrará información del progreso a medida que elimina del sistema el software de VirusScan. Cuando haya finalizado, haga clic en **Finalizar** para cerrar el panel del asistente.

Eliminación de virus del sistema 3

Si sospecha que puede tener un virus

En primer lugar, no se asuste. Aunque no son inocuos, la *mayoría* de los virus que pueden infectar el equipo no destruyen datos ni gastan bromas ni dejan el equipo inutilizable. Incluso los virus comparativamente poco comunes que llevan una carga destructiva sólo liberan sus efectos dañinos en respuesta a un suceso que lo ha desencadenado. En la mayoría de los casos, salvo que realmente tenga evidencia de que se haya activado una carga destructiva, dispondrá de tiempo suficiente para tratar correctamente la infección. No obstante, la mera presencia de estos pequeños retazos de código informático no deseado puede interferir en el funcionamiento normal del equipo, consumir recursos del sistema o tener otros efectos no deseados, por lo que deberá tomarlos en serio y asegurarse de eliminarlos cuando los detecte.

Un segundo aspecto que es preciso tener en cuenta es que el comportamiento extraño del equipo, los bloqueos inexplicables del sistema y otros sucesos impredecibles pueden tener un origen distinto de la infección por virus. Si cree que puede tener un virus en el equipo debido a problemas como los que se mencionan anteriormente, es probable que la exploración no dé los resultados esperados, pero le ayudará a eliminar una posible causa de los problemas.

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

Cuando instala el software de VirusScan, el programa de instalación inicia la aplicación VirusScan para que examine la memoria del equipo y los sectores de arranque del disco duro con el fin de comprobar que se podrán copiar los archivos de forma segura en el disco duro sin riesgo de que se infecten. Si la aplicación no detecta virus, continúa la instalación y, a continuación, explora el sistema completamente tan pronto como reinicia el equipo. Los virus que infectan archivos y que no se cargan en la memoria del equipo o se ocultan en los bloques de arranque del disco duro pueden estar al acecho en cualquier parte del sistema.

Si la aplicación VirusScan detecta un virus durante la instalación, tendrá que eliminarlo del sistema antes de instalar el programa.

IMPORTANTE: Para garantizar la máxima seguridad, deberá seguir este mismo procedimiento si un componente de VirusScan detecta un virus en la memoria del equipo una vez finalizada la instalación.

Si el software de VirusScan detecta una infección durante la instalación, siga estos pasos:

1. Salga inmediatamente del programa de instalación y apague el equipo.

   Asegúrese de que el equipo está completamente apagado. *No* presione CTRL+ALT+SUPR ni reinicialice el equipo para reiniciar el sistema, ya que algunos virus pueden quedar intactos durante este tipo de reinicio "en caliente".

2. Si durante la instalación ha creado un disco de emergencia de VirusScan o si la copia de VirusScan incluía uno, bloquee el disco y, a continuación, insértelo en la unidad de disquete.

   - **NOTA:** Si la copia de software de VirusScan no incluía un disco de emergencia o si no pudo crear un disco de este tipo durante la instalación, deberá crear uno en un equipo *que no esté infectado.*

3. Espere al menos 15 segundos y, a continuación, vuelva a iniciar el equipo.

   - **NOTA:** Si ha configurado la BIOS del equipo para que busque, en primer lugar, el código de inicio en la unidad C:, debería cambiar la configuración de la BIOS para que primero busque en la unidad A: o B: . Consulte la documentación del hardware para obtener más información acerca de la configuración de la BIOS.

   Después de que se inicie el equipo, el disco de emergencia ejecutará un archivo de procesamiento por lotes que le guiará por una operación de exploración de emergencia. El archivo de procesamiento por lotes primero le pregunta si desea realizar un ciclo en la alimentación del equipo.

4. Escriba y para seguir y, a continuación, vaya al paso 7. Si no lo ha hecho ya, escriba n y apague completamente el equipo para comenzar de nuevo.

   A continuación el archivo de procesamiento por lotes le indicará que va a comenzar una operación de exploración.

5. Lea el mensaje que se muestra en la pantalla y presione cualquier tecla del teclado para continuar.

   El disco de emergencia cargará los archivos que necesita para realizar la operación de exploración en memoria. Si el equipo dispone de memoria extendida, los archivos de la base de datos se cargarán en dicha memoria para que se ejecute con mayor rapidez.

BOOTSCAN.EXE, el explorador de línea de comandos incluido en el disco de emergencia, llevará a cabo 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, así como otros puntos susceptibles a la infección en todos los discos duros locales del equipo.

- **NOTA:** McAfee VirusScan Software recomienda encarecidamente no interrumpir el explorador BOOTSCAN.EXE durante la operación de exploración. El disco de emergencia no detectará virus de macros, de secuencias de comandos o de programas denominados caballos de Troya, pero sí detectará los virus que infectan los archivos comunes y los sectores de arranque.

Si BOOTSCAN.EXE encuentra un virus, intentará limpiar el archivo infectado. Si no puede, denegará el acceso al archivo y continuará con la operación de exploración. Después de finalizar la exploración, aparecerá en la pantalla un informe con las acciones que realizó en cada disco duro. El informe contendrá la siguiente información:

- El número de archivos que el explorador ha examinado
- El número de esos archivos que están limpios o sin virus
- El número de archivos que contienen posibles virus
- El número de archivos que el explorador ha limpiado
- El número de archivos del sector de arranque y del MBR que el explorador ha examinado
- El número de archivos del sector de arranque y del MBR que contienen posibles virus

Si el explorador detecta un virus, emitirá un sonido e informará sobre el nombre y la ubicación del virus en la pantalla.

6. Cuando el explorador termine de examinar el disco duro, extraiga el disco de emergencia de la unidad de disquete y, a continuación, vuelva a apagar el equipo.
7. Una vez que BOOTSCAN.EXE haya terminado la comprobación del sistema, podrá:

- **Volver a trabajar con el equipo.** Si BOOTSCAN.EXE no ha detectado ningún virus ni ha limpiado los archivos infectados que ha encontrado, extraiga el disco de emergencia de la unidad de disquete y reinicie el equipo. Si pensaba instalar el software de VirusScan en el equipo pero interrumpió el proceso cuando el programa de instalación encontró un virus, ahora puede continuar con la instalación.
- **Tratar de limpiar o eliminar los archivos infectados.** Si BOOTSCAN.EXE ha encontrado un virus que no ha podido eliminar, identificará los archivos infectados y le indicará que no ha podido limpiarlos o que no dispone del limpiador adecuado para ese virus en concreto.

El siguiente paso consiste en buscar y eliminar el archivo o archivos infectados. En este caso, tendrá que recuperar los archivos eliminados a partir de las copias de seguridad. Compruebe si los archivos de las copias de seguridad también contienen virus. Asegúrese también de utilizar la aplicación VirusScan, en cuanto pueda, para explorar completamente el sistema y comprobar que no contiene virus.

Cuándo explorar en busca de virus

Mantener un entorno informático seguro significa explorarlo periódicamente en busca de virus. Según la frecuencia con que intercambie disquetes con otros usuarios, comparta archivos a través de la red de área local o se comunique con otros equipos a través de Internet, la "periodicidad" de la exploración puede significar tan poco como una vez al mes o tan a menudo como varias veces al día. Entre los hábitos correctos se incluyen, además, la exploración antes de hacer una copia de seguridad de los datos, antes de instalar un programa o versión nuevos, especialmente si se ha descargado el software de otro equipo, y al encender o apagar el equipo después de una sesión. Utilice el explorador VShield para examinar la memoria del equipo y mantener un nivel constante de vigilancia entre las operaciones de exploración. En la mayoría de los casos, esto bastará para proteger la integridad del sistema.

Si se conecta a Internet con frecuencia o descarga archivos a menudo, es posible que desee realizar con regularidad operaciones de exploración adicionales con tareas basadas en determinados sucesos. Utilice la Consola de VirusScan para programar una serie de tareas de exploración que le ayudarán a supervisar el sistema en los puntos más sensibles a la entrada de virus, como por ejemplo:

- Al insertar un disquete en la unidad de disquete del equipo
- Al iniciar una aplicación o abrir un archivo
- Al conectarse o asignar una unidad de red al sistema

Cómo reconocer que el equipo no está infectado

Los equipos personales han evolucionado, en su breve vida, hasta convertirse en complejas máquinas que utilizan un software cada vez más complicado. Ni siquiera los defensores de los primeros equipos informáticos con una visión de futuro más amplia podrían haber imaginado las tareas para las que los trabajadores, científicos, etc., han utilizado la velocidad, flexibilidad y potencia del equipo informático moderno. Sin embargo, esta potencia tiene un precio: abundan los conflictos entre el hardware y el software, fallan las aplicaciones y los sistemas operativos y muchos otros problemas pueden aparecer en los lugares más insospechados. En algunos casos, estos fallos pueden tener efectos similares a los que produce un virus con una carga destructiva. Otros fallos de los equipos parecen desafiar cualquier intento de explicación o diagnóstico, por lo que los usuarios frustrados acaban culpando a los virus, quizá como último recurso.

Sin embargo, dado que los virus suelen dejar rastro, normalmente podrá descartar la infección vírica como causa del fallo del equipo de manera rápida y sencilla. Al ejecutar una operación de exploración completa con VirusScan se detectarán todas las variantes de virus conocidas que pueden infectar el equipo, además de un número elevado de las que no tienen un nombre conocido o un comportamiento definido. Aunque esto no sirva de mucha ayuda si el fallo del sistema se debe a un conflicto de interrupción, le permitirá eliminar una de las posibles causas del problema. Con estos datos, puede proceder a resolver los problemas del sistema con una utilidad completa de diagnóstico del sistema.

El problema se complica con la confusión que producen los programas que se comportan como virus, las trampas de los virus y las violaciones reales de la seguridad. El software antivirus simplemente no puede detectar o reaccionar ante dichos agentes destructivos tales como los programas denominados caballo de Troya que no han aparecido con anterioridad, o la percepción de que un virus existe cuando de hecho no es así.

La mejor manera de establecer si el fallo del equipo se debe al ataque de un virus es ejecutar una exploración completa y analizar los resultados. Si la aplicación VirusScan no notifica la existencia de una infección a causa de virus, las posibilidades de que el problema se deba a uno son muy pequeñas, por lo que debe buscar otras causas. Es más, aún en el supuesto caso de que la aplicación VirusScan no detecte un virus de macro o de otro tipo que, de hecho, haya infectado el sistema, las posibilidades de que se produzcan daños graves son relativamente pequeñas. No obstante, puede confiar en los investigadores de McAfee VirusScan para identificar y aislar el virus y, a continuación, actualizar enseguida el software de VirusScan para que pueda detectar y, si es posible, eliminar el virus cuando lo vuelva a encontrar.

Identificación de falsas detecciones

Se produce una falsa detección cuando el software de VirusScan envía un mensaje de alerta de virus o crea una entrada en el archivo de registro para identificar un virus que en realidad no existe. Existen más posibilidades de que se produzca una falsa alarma si utiliza software antivirus de distintas marcas, ya que algunos de estos programas almacenan en la memoria las firmas de códigos que utilizan, sin protegerlas.

Cuando se genera un mensaje de alerta o una entrada de registro, la acción más segura es tratarlo como si fuera un virus auténtico y realizar el procedimiento adecuado para eliminarlo del sistema. No obstante, si cree que un componente de VirusScan ha generado una falsa detección, por ejemplo, si ha marcado como infectado un archivo que ha utilizado durante años sin problemas, asegúrese de que no se encuentra en ninguna de estas situaciones antes de llamar al servicio de soporte técnico de McAfee VirusScan:

- **Está ejecutando varios programas antivirus.** En este caso, los componentes de VirusScan pueden detectar firmas de códigos no protegidas que otro programa utiliza y notificarlas como virus. Para evitar este problema, configure el equipo de manera que ejecute un solo programa antivirus y, a continuación, apáguelo y desconéctelo. Espere unos segundos y enciéndalo de nuevo para que el sistema pueda eliminar de la memoria las cadenas de firma de código de los demás programas.
- **Uno de sus chips BIOS cuenta con una función antivirus.** Algunos chips BIOS disponen de funciones antivirus que pueden activar falsas detecciones cuando se ejecuta VirusScan. Consulte la guía del usuario del equipo para obtener información sobre el funcionamiento de estas funciones y, si es necesario, su desactivación.
- **Dispone de un equipo Hewlett-Packard o Zenith antiguo.** Algunos modelos antiguos de estos fabricantes modifican el sector de arranque del disco duro cada vez que se pone en marcha el sistema. Los componentes de VirusScan pueden identificar estas modificaciones como virus, aunque no lo sean. Consulte la guía del usuario del equipo para saber si tiene un código de arranque automodificable. Para resolver este problema, utilice el explorador línea de comandos de VirusScan para añadir información de validación en los archivos de inicio. De esta forma, no guardará información del sector de arranque ni del registro de arranque principal.
- **El software está protegido contra copia.** Según el tipo de protección contra copia utilizado, los componentes de VirusScan pueden detectar un virus en el sector de arranque o en el registro de arranque principal de disquetes u otros soportes.

Si no se da ninguna de estas situaciones, póngase en contacto con el servicio de soporte técnico de McAfee VirusScan o envíe un mensaje de correo electrónico a virus_research@nai.com con una explicación detallada del problema.

Respuesta a los virus o software perjudicial

Puesto que el software de VirusScan consta de distintos programas y cualquiera de ellos puede estar activo en un momento concreto, las posibles respuestas a las infecciones por virus u otro software perjudicial dependerán del programa que haya detectado el objeto dañino, de la configuración de respuesta de dicho programa y de otras circunstancias. Las siguientes secciones proporcionan una descripción general de las respuestas predeterminadas disponibles en cada componente de programa. Para obtener información sobre otras posibles respuestas, consulte el capítulo en el que se describe cada componente de forma detallada.

Respuesta del explorador VShield cuando detecta software perjudicial

El explorador VShield está compuesto de cuatro módulos relacionados que proporcionan protección automática continua en segundo plano contra los virus, los objetos de Java y ActiveX perjudiciales y los sitios Web peligrosos. Un quinto módulo controla las opciones de seguridad de los otros cuatro. Puede configurar y activar cada módulo por separado o utilizarlos de forma conjunta para obtener la máxima protección. Dado que cada módulo detecta objetos diferentes o explora distintos puntos de entrada de virus, cada uno de ellos dispone de un conjunto de respuestas predeterminadas diferente.

Respuesta cuando el módulo Exploración de sistema detecta un virus

La forma en la que este módulo reacciona cuando encuentra un virus depende del sistema operativo que ejecute el equipo y, en el caso de los sistemas Windows 95 y Windows 98, depende de la opción de símbolo del sistema seleccionada en la página Acción del módulo.

De forma predeterminada, en los sistemas Windows 95 y Windows 98, este módulo busca virus cada vez que ejecuta, copia, crea o cambia el nombre de un archivo en el sistema, o bien cuando lee de un disquete. En los sistemas Windows NT Workstation versión 4.0 y Windows 2000 Professional, el módulo Exploración de sistema busca virus cada vez que el sistema u otro equipo lee archivos del disco duro o disquete, o escribe archivos en ellos.

Al explorar los archivos de este modo, puede servir de copia de seguridad en el caso de que otro de los módulos de VShield no detecte ningún virus la primera vez que entre en el sistema. En la configuración inicial, el módulo denegará el acceso a cualquier archivo infectado que encuentre, independientemente de la versión de Windows que se ejecute en el equipo. De igual manera, mostrará un mensaje de alerta que le preguntará qué desea hacer con el virus. Las opciones de respuesta que aparecen en este cuadro de diálogo proceden de las opciones predeterminadas o las seleccionadas en la página Acción del módulo Exploración de sistema.

Mientras que el cuadro de diálogo espera la respuesta, el equipo seguirá realizando cualquier otra tarea que ejecute en segundo plano.

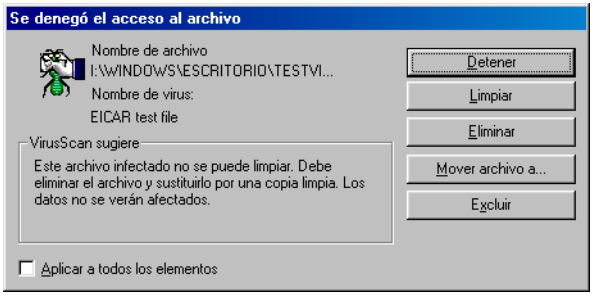

Figura 3-1. Opciones iniciales de respuesta del módulo Exploración de sistema

Si el equipo ejecuta Windows 95 o Windows 98, puede hacer que se muestre un mensaje de alerta de virus diferente. Si selecciona **BIOS** en el área Tipo de comando en la página Acción del módulo Exploración de sistema, en su lugar aparecerá una advertencia a toda pantalla que ofrece las opciones de respuesta.

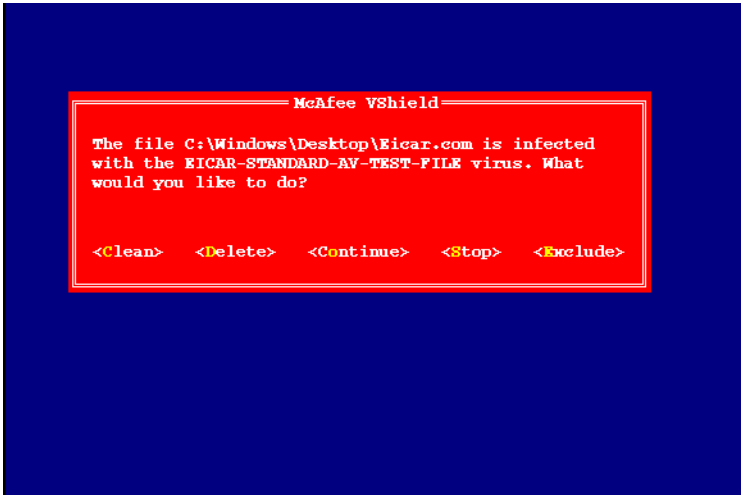

Figura 3-2. Advertencia a toda pantalla: opciones de respuesta de Exploración de sistema

Este mensaje de alerta hace que el sistema se pare completamente mientras espera la respuesta. No se ejecutarán en el sistema otros programas u operaciones del sistema hasta que seleccione una de las opciones de respuesta que aparecen.

El tipo de comando de la BIOS también permite sustituir la opción **Continuar** por la opción **Mover archivo**. Para llevarlo a cabo, active la casilla de verificación **Continuar acceso** de la página Acción del módulo.

- **NOTA:** La casilla de verificación Continuar acceso no estará disponible si el equipo ejecuta Windows NT Workstation versión 4.0 o Windows 2000, o si selecciona el tipo de comando **GUI** en los sistemas Windows 95 y Windows 98.

Para emprender una de las acciones enumeradas en un mensaje de alerta, haga clic en un botón del cuadro de diálogo Se denegó el acceso al archivo, o escriba la letra resaltada en amarillo cuando aparezca la advertencia a toda pantalla. Para que se aplique la misma respuesta a todos los archivos infectados que encuentre el módulo Exploración de sistema durante esta operación de exploración, active la casilla de verificación **Aplicar a todos los elementos** del cuadro de diálogo. Esta opción no estará disponible en el mensaje de alerta a toda pantalla.

Las opciones de respuesta son:

- **Limpiar el archivo.** Haga clic en **Limpiar** en el cuadro de diálogo o escriba C cuando vea la advertencia a toda pantalla para indicar así al módulo Exploración de sistema que intente eliminar el código de virus del archivo infectado. Si el módulo lo consigue, restaurará el archivo a su estado original y registrará la acción en el archivo de registro.

  Si el módulo no puede limpiar el archivo, bien porque no dispone de la herramienta de eliminación o porque el virus ha dañado el archivo más allá de su posible reparación, dejará constancia del resultado en el archivo de registro, pero no realizará ninguna otra acción. En la mayoría de los casos, tendrá que eliminar los archivos infectados y recuperarlos a partir de las copias de seguridad.

- **Eliminar el archivo.** Haga clic en **Eliminar** en el cuadro de diálogo o escriba D cuando vea la advertencia a toda pantalla para indicar así al módulo Exploración de sistema que elimine el archivo infectado de inmediato. De forma predeterminada, el módulo toma nota del nombre del archivo infectado en el archivo de registro para facilitarle un registro de los archivos infectados que identifica. Puede recuperar los archivos eliminados de las copias de seguridad.

- **Mover el archivo a otra ubicación.** Haga clic en **Mover archivo a** en el cuadro de diálogo. Se abrirá una ventana de exploración que podrá utilizar para buscar la carpeta de cuarentena o cualquier otra carpeta que desee utilizar para aislar los archivos infectados. Una vez seleccionada la carpeta, el módulo Exploración de sistema mueve inmediatamente el archivo a dicha carpeta. Esta opción no aparece en la advertencia a toda pantalla.

- **Continuar la exploración.** Escriba O cuando aparezca la advertencia a toda pantalla para indicar al módulo Exploración de sistema que le permita seguir trabajando con el archivo y que no adopte medida alguna. Generalmente, utilizará esta opción para saltarse los archivos que sabe que no tienen virus. Si la opción de generación de informes está activada, el módulo anotará cada incidente en el archivo de registro. Esta opción no está disponible en el cuadro de diálogo Se denegó el acceso al archivo.
- **Detener exploración.** Haga clic en **Detener** en el cuadro de diálogo, o escriba S cuando aparezca la advertencia a toda pantalla para indicar así al módulo Exploración de sistema que le deniegue el acceso al archivo y que no emprenda ninguna otra acción. Al prohibir el acceso al archivo se evita que nadie pueda abrir, guardar o cambiar de nombre el archivo. Para continuar, debe hacer clic en **Aceptar**. Si la opción de generación de informes está activada, el módulo anotará cada incidente en el archivo de registro.
- **Excluir el archivo de las operaciones de exploración.** Haga clic en **Excluir** en el cuadro de diálogo, o escriba E cuando aparezca la advertencia a toda pantalla para indicar al módulo Exploración de sistema que excluya este archivo de futuras operaciones de exploración. Generalmente, utilizará esta opción para saltarse los archivos que sabe que no tienen virus.

Respuesta cuando el módulo Exploración de correo electrónico detecta un virus

---

NOTA: Esta función sólo se aplica a los mensajes de correo electrónico del servidor de Exchange.

Este módulo explora los mensajes de correo electrónico que recibe a través de los sistemas de correo electrónico corporativos, tales como cc:Mail y Microsoft Exchange. En su configuración inicial, el módulo le pide que seleccione una de las cinco opciones de respuesta que muestra cuando detecta un virus.

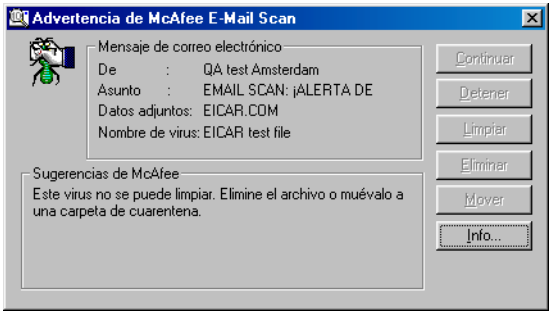

Figura 3-3. Opciones de respuesta del módulo Exploración de correo electrónico

Haga clic en el botón correspondiente a la respuesta deseada. Podrá elegir entre las siguientes opciones:

- **Detener**. Haga clic en este botón para detener la operación de exploración de forma inmediata. El módulo Exploración de correo electrónico registrará cada detección en el archivo de registro, pero no realizará otra acción ante el virus.
- **Limpiar**. Haga clic en este botón para que el módulo Exploración de correo electrónico intente eliminar el código del virus del archivo infectado. Si no consigue limpiar el archivo, bien porque no dispone de la herramienta de eliminación o porque el virus ha dañado el archivo más allá de su posible reparación, tomará nota del incidente en el archivo de registro y sugerirá respuestas alternativas. En el ejemplo que se muestra en la figura 3-3, el módulo no ha conseguido limpiar el archivo de prueba EICAR, un falso "virus" escrito específicamente para probar si el software antivirus instalado funciona correctamente. En este caso, la opción **Limpiar** no está disponible. En la mayoría de los casos, tendrá que eliminar los archivos infectados y recuperarlos a partir de las copias de seguridad.
- **Eliminar**. Haga clic en este botón para eliminar inmediatamente el archivo del sistema. De forma predeterminada, el módulo Exploración de correo electrónico registrará el nombre del archivo infectado en el registro para que pueda recuperarlo a partir de la copia de seguridad.
- **Mover archivo a**. Haga clic en este botón para abrir un cuadro de diálogo que le permitirá localizar la carpeta de cuarentena u otra carpeta adecuada. Una vez localizada la carpeta, haga clic en **Aceptar** para mover el archivo a dicha ubicación.
- **Excluir**. Haga clic en este botón para evitar que el módulo Exploración de correo electrónico marque este archivo como virus en las próximas operaciones de exploración. Si copia este archivo en el disco duro, evitará también que el módulo Exploración de sistema detecte el archivo como virus.

Cuando seleccione la acción, el módulo Exploración de correo electrónico la implementará inmediatamente y agregará un aviso en la parte superior del mensaje de correo electrónico que contenga un archivo adjunto infectado. Este aviso incluye el nombre del archivo adjunto infectado, el nombre del virus y describe la acción que el módulo ha realizado en respuesta.

Para que se aplique la misma respuesta a todos los archivos infectados que encuentre el módulo Exploración de correo electrónico durante esta operación de exploración, active la casilla de verificación **Aplicar a todos los elementos** del cuadro de diálogo.

Respuesta cuando el módulo Exploración de transferencias detecta un virus

Este módulo explora los mensajes de correo electrónico y otros archivos que recibe de Internet a través del visualizador de Web o de programas cliente de correo electrónico tales como Eudora Light, Netscape Mail, Outlook Express, etc. *No* detectará los archivos que se descarguen con aplicaciones cliente FTP, aplicaciones de terminal o a través de canales similares. En su configuración inicial, el módulo le pide que seleccione una de las tres opciones de respuesta que muestra cuando detecta un virus (figura 3-4). Una cuarta opción le facilita información adicional.

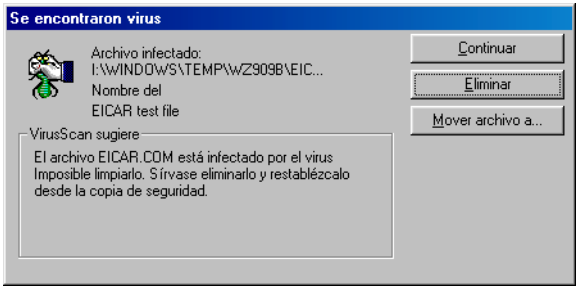

Figura 3-4. Opciones de respuesta del módulo Exploración de transferencias

Haga clic en el botón correspondiente a la respuesta deseada. Podrá elegir entre las siguientes opciones:

- **Continuar**. Haga clic en esta opción para indicar al módulo Exploración de transferencias que no realice ninguna acción y continúe con la exploración. El módulo proseguirá hasta que detecte otro virus en el sistema o finalice la operación de exploración. Generalmente, utilizará esta opción para saltarse los archivos que sabe que no tienen virus o en caso de que piense dejar el equipo sin vigilancia mientras descarga correo electrónico u otros archivos. El módulo anotará todos los incidentes en el archivo de registro.
- **Eliminar**. Haga clic en esta opción para indicarle al módulo Exploración de transferencias que elimine el archivo infectado o archivo adjunto del mensaje de correo electrónico que ha recibido. De forma predeterminada, el módulo toma nota del nombre del archivo infectado en el archivo de registro.
- **Mover**. Haga clic en esta opción para indicar al módulo Exploración de transferencias que mueva el archivo infectado al directorio de cuarentena seleccionado en la página de propiedades Acción del módulo.

Cuando seleccione la acción, el módulo Exploración de transferencias la implementará inmediatamente y agregará un aviso en la parte superior del mensaje de correo electrónico que contenga un archivo adjunto infectado. Este aviso incluye el nombre del archivo adjunto infectado, el nombre del virus y describe la acción que el módulo ha realizado en respuesta.

Respuesta cuando el módulo Filtro de Internet detecta un virus

Este módulo busca Clases de Java o controles ActiveX hostiles cada vez que visita un sitio Web o descarga archivos de Internet. También puede utilizarlo para impedir que su visualizador se conecte a sitios de Internet peligrosos. En su configuración inicial, el módulo le preguntará siempre que encuentre un objeto potencialmente peligroso si desea **Denegar** el acceso de dicho objeto al sistema o **Continuar** y permitirle el acceso. Le ofrecerá la misma posibilidad cuando intente conectarse a un sitio Web potencialmente peligroso (figura 3-5).

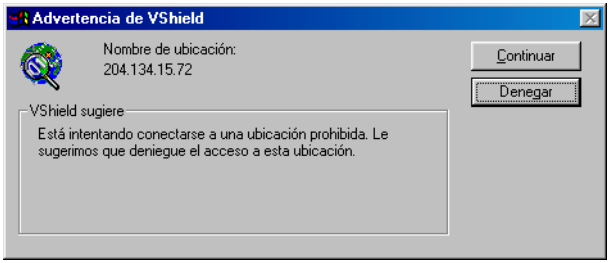

Figura 3-5. Opciones de respuesta de Filtro de Internet

Respuesta cuando la aplicación VirusScan detecta un virus

Cuando ejecuta una operación de exploración por primera vez con la aplicación VirusScan, analizará todos los archivos de la unidad C: que puedan contener un virus. De este modo obtiene un nivel básico de protección que puede ampliar configurando el software de VirusScan de acuerdo a sus propias necesidades.

Con esta configuración inicial, el programa le pedirá una respuesta cuando detecte un virus (figura 3-6).

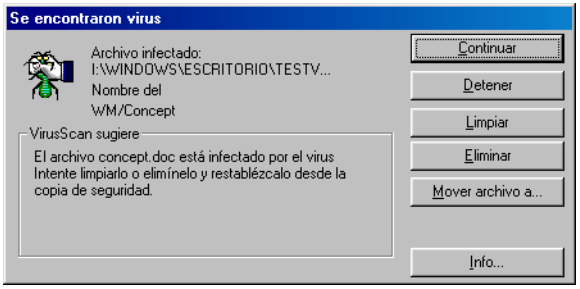

Figura 3-6. Opciones de respuesta de VirusScan

Para tratar la infección, haga clic en uno de los botones que aparecen. Puede indicar a la aplicación VirusScan una de las siguientes opciones:

- **Continuar.** Haga clic en este botón para continuar con la operación de exploración y para que la aplicación muestre todos los archivos infectados que encuentre en la parte inferior de la ventana principal (figura 3-7) y registre cada detección en el archivo de registro, pero sin emprender ninguna acción contra el virus. Una vez que la aplicación ha terminado de examinar el sistema, puede hacer clic con el botón derecho del ratón en cada uno de los archivos que aparecen en la ventana principal y seleccionar una respuesta individual en el menú de acceso directo que aparece.

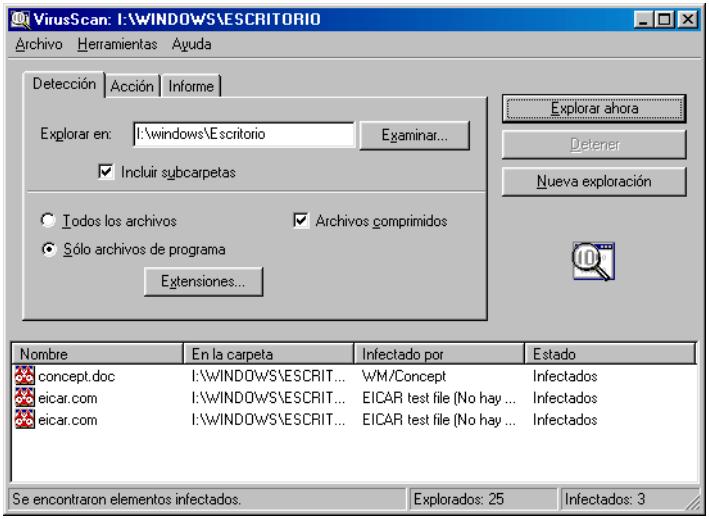

Figura 3-7. Ventana principal de VirusScan

- **Detener.** Haga clic en este botón para detener la operación de exploración de forma inmediata. La aplicación VirusScan mostrará en la parte inferior de su ventana principal los archivos infectados que haya localizado (figura 3-7) y los anotará en el archivo de registro, pero sin emprender ninguna otra acción contra el virus. Haga clic con el botón derecho del ratón en cada uno de los archivos infectados que aparecen en la ventana principal y seleccione una respuesta individual en el menú de acceso directo que aparece.
- **Limpiar.** Haga clic en este botón para que la aplicación VirusScan intente eliminar el código de virus del archivo infectado. Si no consigue limpiar el archivo, bien porque no dispone de la herramienta de eliminación o porque el virus ha dañado el archivo más allá de su posible reparación, tomará nota del incidente en el archivo de registro y sugerirá respuestas alternativas.

  En el ejemplo que se muestra en la figura 3-6, la aplicación no ha conseguido limpiar el archivo de prueba EICAR, un falso "virus" escrito específicamente para probar si el software antivirus instalado funciona correctamente. En este caso, la opción **Limpiar** no está disponible. En la mayoría de los casos, tendrá que eliminar los archivos infectados y recuperarlos a partir de las copias de seguridad.
- **Delete (eliminar).** Haga clic en este botón para eliminar inmediatamente el archivo del sistema. De forma predeterminada, la aplicación VirusScan registrará el nombre del archivo infectado en el archivo de registro para que pueda recuperarlo a partir de la copia de seguridad.
- **Mover archivo a.** Haga clic en esta opción para abrir un cuadro de diálogo que le permita localizar la carpeta de cuarentena u otra carpeta adecuada. Una vez localizada la carpeta, haga clic en **Aceptar** para mover el archivo a dicha ubicación.
- **Info.** Haga clic aquí para conectarse a la Biblioteca de información sobre virus de McAfee VirusScan. Si selecciona esta opción no se llevará a cabo ninguna acción contra el virus que ha detectado la aplicación.

Respuesta cuando la extensión Exploración de correo electrónico detecta un virus

---

NOTA: Esta función sólo se aplica a los mensajes de correo electrónico del servidor de Exchange.

La extensión Exploración de correo electrónico incluida en el software de VirusScan le permite explorar los mensajes de correo electrónico de entrada de Microsoft Exchange o Microsoft Outlook para detectar virus si así lo desea. Puede activar este componente desde el cliente de correo electrónico y utilizarlo como complemento de la exploración continua en segundo plano del

correo electrónico del módulo Exploración de correo electrónico de VShield. El módulo Exploración de correo electrónico también le permite limpiar los archivos adjuntos infectados o detener la operación de exploración, una posibilidad que sirve de complemento a la supervisión continua que proporciona este módulo. En su configuración inicial, el módulo Exploración de correo electrónico le solicita que proporcione una respuesta cuando detecta un virus.

Para tratar la infección, haga clic en uno de los botones que aparecen. La extensión Exploración de correo electrónico dispone de las siguientes opciones:

- **Continuar**. Haga clic en este botón para que la extensión Exploración de correo electrónico continúe con la operación de exploración, muestre todos los archivos infectados que encuentre en la parte inferior de la ventana principal (figura 3-8) y anote cada detección en el archivo de registro, pero sin emprender ninguna acción contra el virus. La extensión continuará hasta que detecte otro virus en el sistema o finalice la operación de exploración. Una vez que haya terminado de examinar el sistema, puede hacer clic con el botón derecho del ratón en cada uno de los archivos que aparecen en la ventana principal y seleccionar una respuesta individual en el menú de acceso directo que aparece.

- **Detener**. Haga clic en este botón para detener la operación de exploración de forma inmediata. La extensión Exploración de correo electrónico mostrará en la parte inferior de la ventana principal (figura 3-8) los archivos infectados que haya localizado y anotará cada detección en el archivo de registro, pero sin emprender ninguna otra acción contra el virus. Haga clic con el botón derecho del ratón en cada uno de los archivos infectados que aparecen en la ventana principal y seleccione una respuesta individual en el menú de acceso directo que aparece.

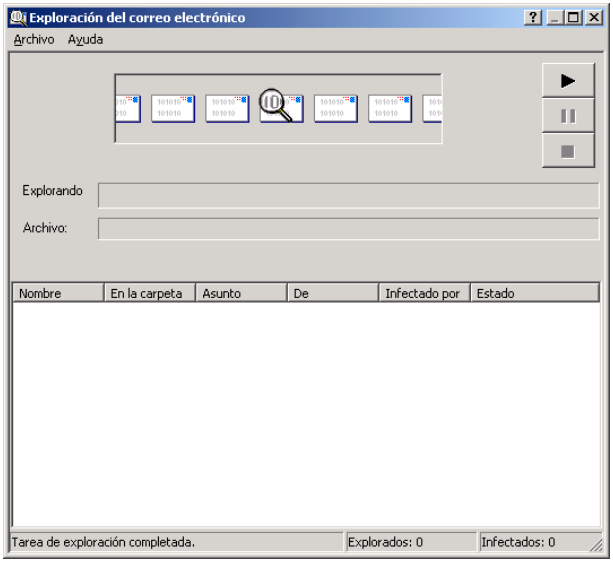

Figura 3-8. Ventana de la extensión Exploración de correo electrónico

- **Limpiar**. Haga clic en este botón para eliminar el código del virus del archivo infectado. Si la extensión Exploración de correo electrónico no consigue limpiar el archivo, bien porque no dispone de la herramienta de eliminación o porque el virus ha dañado el archivo más allá de su posible reparación, tomará nota del incidente en el archivo de registro y sugerirá respuestas alternativas. En el ejemplo que se muestra en la figura 3-8, **Limpiar** no está disponible. En la mayoría de los casos, tendrá que eliminar los archivos infectados y recuperarlos a partir de las copias de seguridad.
- **Eliminar**. Haga clic en este botón para eliminar el archivo del sistema. De forma predeterminada, la extensión Exploración de correo electrónico, registrará el nombre del archivo infectado en el registro para que pueda recuperarlo a partir de la copia de seguridad.
- **Mover**. Haga clic en este botón para abrir un cuadro de diálogo que le permitirá localizar la carpeta de cuarentena u otra carpeta adecuada. Una vez localizada la carpeta, haga clic en **Aceptar** para mover el archivo a dicha ubicación.
- **Info**. Haga clic aquí para conectarse a la Biblioteca de información sobre virus de McAfee VirusScan. Si selecciona esta opción, la extensión Exploración de correo electrónico no llevará a cabo ninguna acción contra el virus que ha detectado.

Ver la información sobre virus

Al hacer clic en **Info** en cualquiera de los cuadros de diálogo de respuestas de virus se conectará a la Biblioteca de información sobre virus en línea de McAfee VirusScan, en el caso de que disponga en el equipo de conexión a Internet y software para examinar la Web (figura 3-9).

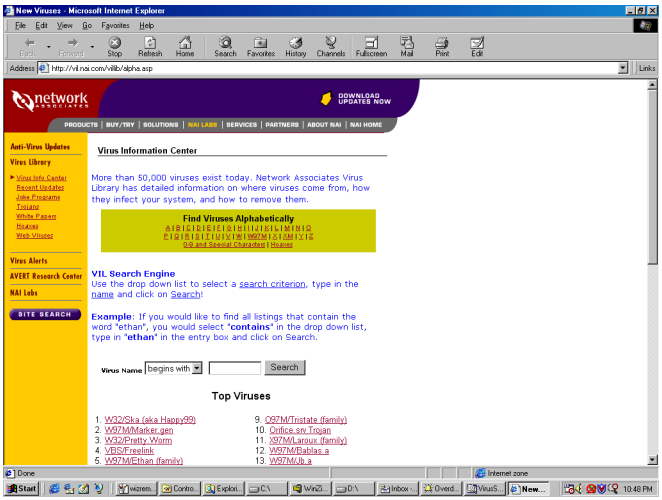

Figura 3-9. Página Biblioteca de información sobre virus de McAfee VirusScan

La Biblioteca de información sobre virus es una colección de documentos que proporciona una descripción general de los virus que el software VirusScan detecta o limpia, así como la información sobre la forma en que el virus infecta y cambia los archivos, y los tipos de cargas destructivas que expande. Este sitio muestra los virus más comunes o peligrosos, proporciona un motor de búsqueda que le permitirá buscar descripciones de virus concretas alfabéticamente o por nombre, y ofrece acceso a los datos técnicos que podrá utilizar para eliminar los virus del sistema.

Para conectarse directamente a la Biblioteca, visite la página:

http://vil.nai.com/villib/alpha.asp

También se puede conectar directamente a la Biblioteca desde la Consola de VirusScan, para ello seleccione **Lista de virus** en el menú **Ver** en la ventana de la Consola.

La Biblioteca está en el sitio Web de McAfee VirusScan AVERT:

http://www.nai.com/asp_set/anti_virus/avert/intro.asp

El sitio Web de AVERT ofrece una gran colección de datos y software relacionados con los virus.

Los ejemplos incluyen:

- Información actual y evaluación de riesgos acerca de las nuevas y activas amenazas de virus
- Herramientas de software que podrá utilizar para ampliar o complementar el software antivirus de McAfee VirusScan
- Direcciones de contacto y otra información para enviar preguntas, ejemplos de virus y otros datos
- Actualizaciones de definiciones de virus que incluyen actualizaciones de versiones beta de archivos .DAT diarias, archivos EXTRA.DAT, archivos .DAT de emergencia actualizados, versiones actuales de motores de exploración, actualizaciones semanales de .DAT y SuperDAT y nuevos archivos de definiciones de virus de incrementos (.UPD)
- Software beta y de "primera prueba"

Ver la información de archivos

Si hace clic con el botón derecho en un archivo mostrado en la ventana principal de VirusScan o en la ventana del módulo Exploración de correo electrónico (vea la figura 3-8) y, a continuación, selecciona **Información sobre archivo** en el menú de acceso directo que aparece, el software de VirusScan abrirá un cuadro de diálogo de información sobre el elemento infectado donde se muestra el nombre del archivo, el tipo y tamaño en bytes, proporciona las fechas de creación y modificación, y describe sus atributos (figura 3-10).

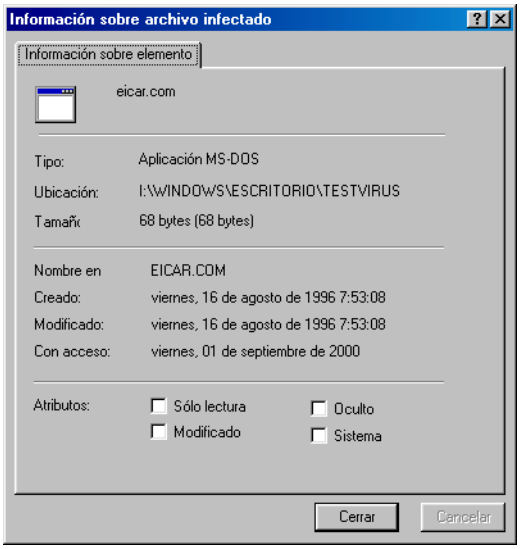

Figura 3-10. Página de propiedades Información sobre archivo infectado

Envío de un ejemplo de virus

Si tiene un archivo que sospecha que contiene virus, o si el sistema falla como consecuencia de una posible infección, pero el software de VirusScan no ha detectado ningún virus, McAfee VirusScan recomienda que envíe una muestra al equipo de investigación antivirus para que la analice. Si lo hace de esta forma, asegúrese de que inicia el sistema en el estado de infección aparente y no desde un disquete limpio.

Existen varios métodos para capturar los ejemplos de virus y enviarlos. En las próximas secciones se exponen los métodos que mejor se adaptan a cada condición en particular.

Uso de la utilidad SendVirus para enviar un archivo de ejemplo

Dado que la mayoría de los virus de última generación tienden a infectar los archivos de documentos y ejecutables, el software de VirusScan incluye SENDVIR.EXE, una utilidad que facilita el envío de un archivo de ejemplo infectado a los investigadores de McAfee VirusScan para analizarlo.

Para enviar un archivo de ejemplo, siga los siguientes pasos:

1. En primer lugar, conéctese a la red o al proveedor de servicios de Internet (ISP) para enviar correos electrónicos, si es necesario. Si está conectado de forma continua a la red o al ISP, omita este paso y vaya al paso 2.

2. Una vez que el archivo esté en cuarentena, inicie la utilidad SendVirus desde la página de cuarentena.
3. Haga doble clic en el archivo para mostrar el primer panel del asistente del Centro de respuestas de AVERT Labs (figura 3-11).

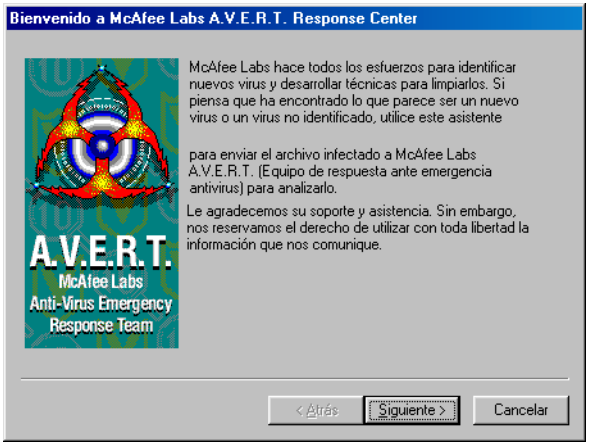

Figura 3-11. Primer panel de SENDVIR.EXE

4. Lea el mensaje de bienvenida y, a continuación, haga clic en **Siguiente>** para continuar.

   Aparecerá el panel del Asistente de información sobre el usuario.

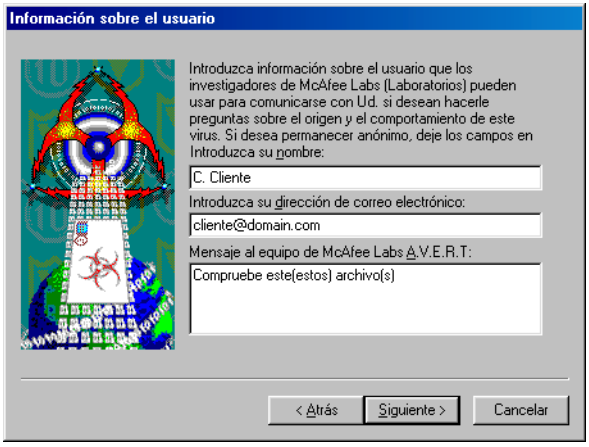

Figura 3-12. Panel Información sobre el usuario

5. Si desea que los investigadores de AVERT se pongan en contacto con relación al envío, escriba en los cuadros de texto proporcionados, su nombre, la dirección de correo electrónico y cualquier mensaje que desee enviar y, a continuación, haga clic en **Siguiente>** para continuar.

- **NOTA:** Si lo prefiere, puede enviar ejemplos de forma anónima; basta con no escribir nada en los cuadros de texto del panel. No está obligado de ninguna forma a proporcionar información en este caso.

Aparecerá el panel Elegir archivos para enviarlos (figura 3-13).

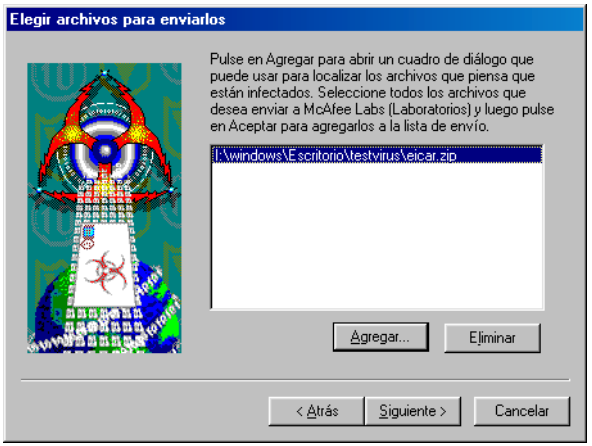

Figura 3-13. Panel Elegir archivos para enviarlos

6. Haga clic en **Agregar** para abrir el cuadro de diálogo que utilizará con el fin de buscar los archivos que pudiesen estar infectados.

   Seleccione tantos archivos como desee enviar para analizar. Para eliminar alguno de los archivos que aparecen en la lista de envío, selecciónelo y, a continuación, haga clic en **Quitar**. Cuando haya seleccionado todos los archivos que desea enviar, haga clic en **Siguiente>** para continuar.

   Aparecerá el panel Elegir opciones de carga (figura 3-14).

Figura 3-14. Panel Elegir opciones de carga

Si el archivo que desea enviar es un documento de Microsoft Office o cualquier otro archivo que contenga información confidencial, active la casilla de verificación **Suprimir mis datos personales del archivo** y, a continuación, haga clic en **Siguiente>** para continuar. De esta forma indica a la utilidad SENDVIR.EXE que elimine del archivo todo excepto las macros o el código ejecutable.

Aparecerá el panel Elegir servicio de correo electrónico (figura 3-15).

Figura 3-15. Panel Elegir servicio de correo electrónico

7. Seleccione el tipo de aplicación de cliente de correo electrónico que tiene instalado en el equipo. Podrá elegir entre las siguientes opciones:

- **Usar correo de Internet de salida**. Haga clic en este botón para enviar el ejemplo mediante el cliente de correo de Protocolo simple de transferencia de correo (SMTP) como Eudora, NetScape Mail o Microsoft Outlook Express. A continuación, escriba el nombre del servidor de correo de salida en el cuadro de texto proporcionado, por ejemplo, correo.dominio.com.
- **Usar Microsoft Exchange**. Haga clic en este botón para enviar el ejemplo mediante el sistema de correo electrónico corporativo. Para utilizar esta opción, el sistema de correo electrónico debe ser compatible con MAPI (Interfaz de programación de aplicaciones de mensajería). Microsoft Exchange, Microsoft Outlook y Lotus cc:Mail versión 8.0 y posterior son ejemplos de dichos sistemas.

8. Haga clic en **Finalizar** para enviar el ejemplo.

- **NOTA:** Aunque los investigadores de McAfee VirusScan agradecen el envío, el recibo del mensaje no les obliga a emprender ninguna acción, proporcionar ninguna solución ni responderle.

SENDVIR.EXE utilizará el cliente de correo electrónico que especificó para enviar el ejemplo. Para que se realice el proceso correctamente debe haberse conectado a la red o al ISP.

Captura de virus del sector de arranque, infección de archivos y virus de macro

Si sospecha que tiene una infección causada por virus, puede recoger un ejemplo del virus y, a continuación, crear una imagen de disquete para enviarla por correo electrónico o enviar el disquete a los investigadores de antivirus de McAfee VirusScan. Los investigadores también se beneficiarán al disponer de los ejemplos de los archivos actuales del sistema en un disquete independiente.

Captura de virus del sector de arranque

Los virus del sector de arranque se ocultan con frecuencia en áreas del disco duro o de los disquetes que normalmente no se pueden ver ni leer. No obstante, puede capturar un ejemplo de un virus del sector de arranque si infecta deliberadamente un disquete con dicho virus.

Para hacerlo, siga los siguientes pasos:

1. Inserte un disquete nuevo y sin formatear en la unidad de disquete.

2. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Programas** y, a continuación, seleccione el **símbolo de MS-DOS** si el equipo ejecuta Windows 95 o Windows 98, o **Interfaz de comandos** o el símbolo del sistema si el equipo ejecuta Windows NT Workstation versión 4.0 o Windows 2000 Professional.

3. Escriba lo siguiente en la línea de comandos:

   ```
   format a: /s
   ```

   Si el sistema se bloquea al intentar formatear el disquete, extráigalo de la unidad de disquete. A continuación, póngale una etiqueta al disquete que indique "Dañado durante formateo infectado como disquete de inicio" y guárdelo.

4. Inserte un disquete nuevo y formateado en la unidad de disquete.

5. Copie los archivos actuales del sistema en ese disco. Para la mayoría de las versiones de DOS, estos archivos incluirán:

   - IO.SYS
   - MSDOS.SYS
   - COMMAND.COM

   Para los sistemas de Windows, copie estos archivos en el mismo disco ya formateado:

   - GDI.EXE
   - KRNL286.EXE o KRNL386.EXE
   - PROGMAN.EXE

6. Póngale una etiqueta al disquete que indique "Contiene archivos infectados" y guárdelo.

Captura de virus que infectan archivos o virus de macro

Si piensa que tiene un virus que infecta archivos o un virus de macro que ha infectado alguno de los archivos de Microsoft Word, Excel o PowerPoint, envíe estos archivos a los investigadores de antivirus de McAfee VirusScan, ya sea con la utilidad SENDVIR.EXE, mediante correo electrónico en forma de imágenes de disquete o por correo en un disquete:

- Si sospecha que un virus ha infectado archivos ejecutables del sistema, copie COMMAND.COM en un disquete formateado y, a continuación, cambie la extensión de los archivos a una extensión no ejecutable.

- Si sospecha que un virus de macro ha infectado los archivos de Microsoft Word, copie NORMAL.DOT y todos los archivos de la carpeta Startup de Microsoft Office al disquete. Si instaló Office en la ubicación predeterminada, encontrará los archivos de inicio de Microsoft Office en:

  C:\Archivos de programa\Microsoft Office\Office\Startup

- Si piensa que un virus de macro ha infectado los archivos de Microsoft Excel, cópielos de C:\Archivos de programa\Microsoft Office\Office\XLSTART al disquete. Incluya todos los archivos que haya instalado en otras ubicaciones de archivos de inicio.

- Si piensa que un virus de macro ha infectado los archivos de PowerPoint, copie el archivo BLANKPRESENTATION.POT de C:\Archivos de programa\Microsoft Office\Templates al disquete.

Imágenes de disquete

Para enviar los archivos almacenados en un disquete que haya creado, puede utilizar una herramienta de McAfee VirusScan AVERT Labs denominada RWFLOPPY.EXE para realizar una imagen de disquete que sintetice la infección. La herramienta RWFLOPPY.EXE no se incluye con el software de VirusScan, pero la puede descargar desde esta página:

http://www.nai.com/asp_set/anti_virus/avert/tools.asp

El sitio de AVERT almacena la herramienta en forma de archivo comprimido .ZIP. Descargue el archivo en el equipo y extráigalo en una carpeta temporal en el disco duro. El paquete .ZIP contiene un archivo de texto breve que explica la sintaxis para usar la utilidad RWFLOPPY.EXE.

NOTA: Si piensa que tiene un virus de sector de arranque, debe utilizar RWFLOPPY para enviar los ejemplos electrónicamente, en caso contrario, debe enviarlos físicamente en un disquete. Si los envía electrónicamente sin utilizar RWFLOPPY, los ejemplos estarán incompletos o no podrán utilizarse, ya que los virus de sector de arranque suelen ocultarse tras los últimos sectores de un disquete y otros programas de creación de imágenes de disquete no pueden obtener estos datos.

Una vez que cree las imágenes de los disquetes que desee enviar, puede enviarlos como archivos adjuntos en un mensaje de correo electrónico a los investigadores antivirus de McAfee VirusScan.

Preparación de los archivos de almacenamiento para enviar

Intente reunir tantos ejemplos de archivos como sea posible en un solo disquete. Para ello, comprima los ejemplos que ha capturado en un disquete en un archivo .ZIP protegido con contraseña. A continuación, se describe un procedimiento que usa la utilidad WinZip:

1. Inicie WinZip.
2. Presione CTRL+N para crear un nuevo archivo de almacenamiento.

   Aparecerá el cuadro de diálogo New Archive.
3. Escriba un nombre para el nuevo archivo y haga clic en **OK**.
4. Presione CTRL+A para agregar archivos al nuevo archivo de almacenamiento.

   Aparecerá el cuadro de diálogo Add.
5. Haga clic en **Password** para abrir el cuadro de diálogo Password.
6. Escriba `INFECTED` en el cuadro de texto de contraseña y haga clic en **OK**.
7. Cuando se lo soliciten, vuelva a escribir la contraseña para comprobar que es igual y haga clic en **OK**.

   Aparecerá el cuadro de diálogo Add With Password.
8. Seleccione los archivos de ejemplos y haga clic en **OK**.

   WinZip aplicará la contraseña escrita a todos los archivos que agregue o extraiga del archivo de almacenamiento. Los archivos que estén protegidos por contraseña aparecerán en la lista de archivos de almacenamiento con un signo más (+) después de los nombres.

   - **NOTA:** Si no protege los ejemplos con la contraseña `INFECTED`, los exploradores antivirus de McAfee VirusScan pueden detectar y limpiar los ejemplos antes de que lleguen a nuestros investigadores.

   ---
9. Adjunte el archivo .ZIP que ha creado en un mensaje de correo electrónico.

Envío de ejemplos a través del correo electrónico

Una vez que ha creado las imágenes de disquete o un archivo de almacenamiento para los ejemplos, envíelos a los investigadores de McAfee VirusScan a una de las siguientes direcciones de correo electrónico:

En Estados Unidos	virus_research@nai.com
En el Reino Unido	vsample@nai.com
En Alemania	virus_research_de@nai.com
En Japón	virus_research_japan@nai.com
En Australia	virus_research_apac@nai.com
En los Paises Bajos	virus_research_europe@nai.com

Incluya la siguiente información en el mensaje:

- Los síntomas que le hicieron sospechar que la máquina estaba infectada
- El producto y la versión con que se detectó el virus, si lo hubo, y los resultados
- Los números de versión de los archivos .DAT y de VirusScan
- Detalles del sistema que puedan ayudar a reproducir el entorno en el que se detectó el virus
- Nombre, empresa, número de teléfono y dirección de correo electrónico, si fuese posible
- Una lista de los elementos que contiene el paquete que envía

Envío de los disquetes por correo

Puede enviar por correo los disquetes que ha creado directamente a los investigadores de antivirus de McAfee VirusScan. McAfee VirusScan aconseja crear un archivo de texto o escribir un mensaje junto con los disquetes que incluya la misma información que enviaría con una imagen de disquete electrónica. Envíe el ejemplo solamente a una dirección de laboratorio de investigación para que pueda recibir una respuesta al problema lo antes posible. Utilice estas direcciones de correo:

En Estados Unidos:

Network Associates, Inc.
Virus Research
20460 NW Von Neumann Drive
Beaverton, OR 97006

En el Reino Unido:

Network Associates, Inc.
Virus Research
Gatehouse Way
Aylesbury, Bucks HP19 3XU
Reino Unido

En Alemania:
Network Associates, Inc.
Virus Research
Luisenweg 40
20537 Hamburg
Alemania

En Japón:
Network Associates, Inc.
Virus Research
9F Toranomon Mori-bldg. 33
3-8-21 Toranomon, Minato-Ku
Tokio
Japón 105-0001

En Australia:
Network Associates, Inc.
Virus Research
500 Pacific Highway, Level 1
St. Leonards, NSW
Sydney
Australia 2065

En Europa:
Network Associates, Inc.
Virus Research
Gatwickstraat 25
1043 GL Amsterdam
Países Bajos

- **NOTA:** Network Associates AVERT Labs guarda todos los ejemplos enviados, pero una vez que envía un ejemplo, AVERT no podrá devolvérselo. AVERT no acepta ni procesa cartuchos Iomega Ditto o Jazz, disquetes Iomega Zip o cualquier otro tipo de medios extraíbles.

Utilización del explorador VShield 4

¿Qué hace el explorador VShield?

Los productos antivirus para equipos individuales de McAfee VirusScan utilizan dos métodos generales para proteger el sistema. El primer método, exploración en segundo plano, funciona constantemente, buscando virus mientras el usuario utiliza el equipo para su trabajo diario. En el producto VirusScan, el explorador VShield realiza esta función. El segundo método permite al usuario iniciar sus propias operaciones de exploración. La aplicación VirusScan es la que realiza generalmente estas tareas.

Dependiendo de su configuración, el explorador VShield puede hacer un seguimiento de cualquier archivo que llegue al sistema o salga de él, ya sea en disquete, a través de la red, en forma de archivos adjuntos que acompañan a los mensajes de correo electrónico o a través de Internet. El explorador busca los virus al abrir, guardar, copiar, renombrar o modificar los archivos, y comprueba la memoria del equipo durante cualquier actividad relacionada con archivos. El explorador se inicia al arrancar el equipo y permanece residente en la memoria hasta que lo cierre o hasta que se apague el sistema. El explorador también incluye funciones opcionales que ofrecen protección contra los subprogramas de Java y controles ActiveX perjudiciales; además, impiden la conexión del equipo a sitios de Internet peligrosos.

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

- **Exploración de sistema**. Este módulo busca virus en el disco duro mientras el usuario trabaja con el equipo. Realiza un seguimiento de los archivos cuando el sistema u otros equipos leen archivos del disco duro o escriben archivos en él. También puede explorar disquetes y unidades de red asignadas al sistema.
- **Exploración de correo electrónico**. Este módulo explora mensajes de correo electrónico y archivos adjuntos a mensajes que se reciben a través de sistemas de correo internos e Internet. Explora el buzón de Microsoft Exchange u Outlook en el servidor de Microsoft Exchange y sistemas de correo electrónico cc:Mail más antiguos.

  Funciona conjuntamente con el módulo Exploración de transferencias para explorar el correo de Internet que llega a través de SMTP (Protocolo simple de transferencia de correo) o POP-3 (Protocolo de oficina de correos).

- **Exploración de transferencias**. Este módulo explora los archivos descargados al sistema desde Internet. Si está activada la opción de correo de Internet en el módulo Exploración de correo electrónico, se incluirán los correos electrónicos y los archivos adjuntos que lleguen a través de sistemas de correo electrónico SMTP o POP3, que incluyen programas cliente de correo electrónico tales como Eudora Pro, Microsoft Outlook Express, NetScape Mail y America Online Mail.
- **Filtro de Internet**. Este módulo busca y bloquea las clases de Java y los controles ActiveX dañinos para que no puedan ser descargados y ejecutados en el sistema cuando se visitan sitios de Internet. También puede impedir que el visualizador se conecte a sitios de Internet potencialmente peligrosos que contienen software perjudicial.

E **IMPORTANTE:** Para utilizar los módulos Exploración de correo electrónico, Exploración de transferencias o Filtro de Internet, primero hay que instalarlos desde la opción de instalación personalizada.

- **Seguridad**. Este módulo proporciona protección con contraseña para los demás módulos de VShield. Se pueden proteger todas o algunas de las páginas de propiedades de los módulos y definir una contraseña para impedir que se realicen cambios no autorizados.

- **NOTA:** Dado que el explorador VShield funciona continuamente, no se deberá instalar o ejecutar más de un explorador VShield en la misma estación de trabajo. De lo contrario, puede que los exploradores interfieran entre sí.

¿Por qué utilizar el explorador VShield?

El explorador VShield posee funciones únicas que lo convierten en parte integral del exhaustivo paquete de seguridad de software antivirus de VirusScan. Entre estas funciones se incluyen:

- **Exploración automática o de acceso**. Este tipo de exploración significa que el explorador busca virus en los archivos que se abren, copian, guardan o modifican de cualquier otra forma, así como en los archivos que se leen y se escriben en disquetes o unidades de red. De este modo, puede detectar y detener los virus en cuanto aparecen en el sistema, incluyendo aquéllos que llegan a través del correo electrónico o como elementos descargados de Internet. Esto significa que puede utilizar el explorador VShield como primera línea de defensa antivirus y como protección entre las diversas operaciones de exploración que realice. El explorador VShield detecta virus en la memoria y en el momento en que intentan ejecutarse en los archivos infectados.

- **Detección y bloqueo de objetos perjudiciales**. El explorador VShield puede evitar que los objetos ActiveX y Java perjudiciales accedan al sistema antes de que se conviertan en una amenaza. Para ello, explora los cientos de objetos que se descargan durante una conexión con la Web u otros sitios de Internet y los archivos adjuntos que se reciben con el correo electrónico. Compara estos elementos con una lista actualizada de objetos perjudiciales y bloquea aquéllos que pueden causar problemas.
- **Filtro de sitios de Internet**. El explorador VShield se distribuye con una lista de sitios Web o de Internet peligrosos que suponen una amenaza para el sistema, normalmente en forma de software perjudicial descargable. Puede añadir cualquier otro sitio al que no quiera que se conecte el software del visualizador, ya sea incluyendo la dirección de protocolo de Internet (IP) o el nombre de dominio.
- **Funcionamiento automático**. El explorador VShield se integra con una amplia gama de software de visualizadores y aplicaciones cliente de correo electrónico. Esto le permite acceder a los archivos adjuntos de correo electrónico y explorarlos en busca de virus antes de que lleguen al equipo.

Si se conecta a Internet o trabaja en una red y deja que este componente funcione en todo momento, podrá mejorar considerablemente su capacidad de detectar y eliminar software perjudicial antes de que tenga la oportunidad de causar daños al sistema.

Compatibilidad con visualizadores y clientes de correo electrónico

El explorador VShield funciona sin problemas con muchos de los visualizadores de Web y software de cliente de correo electrónico más populares disponibles para la plataforma de Windows. Para trabajar con el visualizador, VShield no requiere más configuración que la ya existente para conectar el equipo a Internet. Sin embargo, debe configurar VShield para que funcione correctamente con el software del cliente de correo electrónico.

McAfee VirusScan Software ha sometido a prueba estos visualizadores de Web y ha comprobado que funcionan correctamente con VShield.

- Netscape Navigator versión 3.x
- Netscape Navigator versión 4.0.x (no incluye la versión 4.0.6)
- Microsoft Internet Explorer v3.x, v4.x y v5.x

McAfee VirusScan Software también ha sometido a prueba estos clientes de correo electrónico y ha comprobado que funcionan con el módulo Exploración de transferencias de VShield:

- Microsoft Outlook Express
- Qualcomm Eudora versión 3.x y versión 4.x
- Netscape Mail (incluido en la mayoría de las versiones de Netscape Navigator y Netscape Communicator)
- America Online mail v3.0, v4.0 y v5.0

Para trabajar con el módulo Exploración de correo electrónico de VShield, el sistema de correo electrónico corporativo deberá utilizar el software de cliente de Lotus cc:Mail, Microsoft Exchange o Microsoft Outlook. McAfee VirusScan Software ha sometido a prueba estos clientes y ha comprobado que funcionan correctamente con el módulo Exploración de correo electrónico:

- Microsoft Exchange versiones 4.0, 5.0 y 5.5
- Microsoft Outlook 97 y Outlook 98
- Lotus cc:Mail versiones 6.x, 7.x y 8.x (no compatible con MAPI)

McAfee VirusScan Software no certifica la compatibilidad del software de VShield con otro software de cliente que no esté incluido en la lista anterior.

Activación o inicio del explorador VShield

Al final de la instalación de VirusScan, el programa de instalación pregunta si desea activar el explorador VShield en ese momento. Si la respuesta es afirmativa, el explorador VShield deberá cargarse inmediatamente en la memoria y comenzar a funcionar con un conjunto de opciones predeterminadas que proporcionan una protección antivirus básica. Si la respuesta es negativa, el explorador VShield se cargará automáticamente la próxima vez que reinicie el equipo.

Cuando se inicia por primera vez el explorador VShield, aparece un icono en la bandeja del sistema de Windows que indica los módulos que están activos.

Al principio, el explorador activa únicamente el módulo de Exploración de sistema, que explora virus que llegan al sistema a través de disquetes y otros medios extraíbles, conexiones de red de área local y áreas similares. El módulo Exploración de sistema también explora los archivos que llegan a través del sistema de correo electrónico e Internet, pero para ello requiere la ayuda de los demás módulos de VShield: Exploración de correo electrónico, Exploración de transferencias y Filtro de Internet.

IMPORTANTE: Para utilizar los módulos Exploración de correo electrónico, Exploración de transferencias o Filtro de Internet, primero hay que instalarlos desde la opción de instalación personalizada.

Si el equipo utiliza Windows NT Workstation versión 4.0 o Windows 2000 Professional, el explorador VShield se carga como un servicio de Windows NT denominado McShield, que puede verse en el panel de control de servicios de Windows.

- **NOTA:** McAfee VirusScan Software recomienda no iniciar ni detener el servicio VShield desde el panel de control de Windows. En lugar de ello, se puede detener y reiniciar el explorador desde el panel de control de VirusScan.

Si el equipo utiliza Windows 95 o Windows 98, el explorador se carga de modo que copie un servicio de Windows en esa plataforma. Este servicio no puede verse en la interfaz de usuario de Windows.

Inicio automático del explorador

Si el explorador VShield no se inicia automáticamente, podrá configurar el inicio automático en el panel de control de VirusScan.

Siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.
2. Localice y haga doble clic en el panel de control de VirusScan 

para abrirlo.
3. Haga clic en la ficha Componentes.

Figura 4-1. Panel de control de VirusScan: página Componentes

4. Active la casilla de verificación **Cargar VShield al inicio** que aparece en la parte superior de la página de propiedades Componentes.
5. Haga clic en **Aceptar** para cerrar el panel de control.

Activación del explorador VShield y sus módulos

Una vez instalados todos los componentes de VShield, se puede utilizar cualquiera de los cuatro métodos para activarlos en varias combinaciones.

- **NOTA:** Activar un módulo significa cargarlo en la memoria del equipo para utilizarlo. El explorador VShield puede iniciarse y permanecer activo en la memoria incluso cuando ninguno de sus módulos está activado.

Método 1: Desde el menú de acceso directo de VShield

Siga estos pasos:

1. Haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo.
2. Seleccione **Activación rápida**.
3. Elija uno de los nombres de módulo que aparecen sin marca de verificación. Los nombres de módulo que tienen una marca de verificación están activos. Y los que no tienen marca de verificación están inactivos. Si utiliza este método para activar un módulo, éste permanece activado hasta que reinicia el software de VirusScan o el equipo. En este punto, su estado dependerá de si ha activado o desactivado el módulo en el cuadro de diálogo Propiedades de VirusScan.

Dependiendo de la combinación de módulos que active, el icono de VShield mostrará un estado diferente.

Método 2: Desde el cuadro de diálogo Estado de exploración del sistema

Siga estos pasos:

1. Haga doble clic en el icono de VShield en la bandeja del sistema de Windows para abrir el cuadro de diálogo Estado de exploración de sistema.

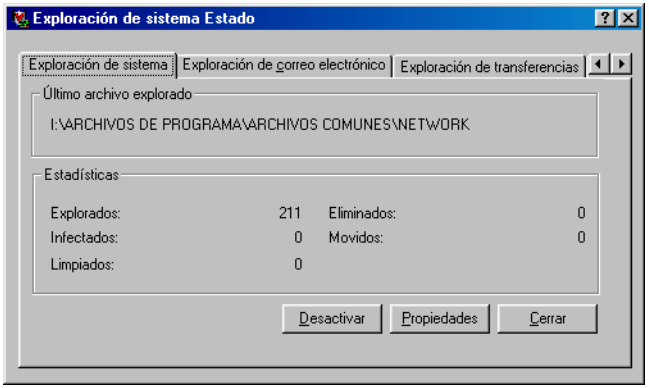

Figura 4-2. Cuadro de diálogo Estado de exploración del sistema

2. Para cada módulo que desee activar, haga clic en la ficha correspondiente y, a continuación, en **Activar**. El mismo botón de la página de propiedades de los módulos activos aparecerá como **Desactivar**.
3. Haga clic en **Cerrar** para cerrar el cuadro de diálogo.

Dependiendo de la combinación de módulos que active, el icono de VShield mostrará un estado diferente.

Método 3: Desde el cuadro de diálogo Propiedades de VShield

Siga estos pasos:

1. Haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo de VShield, elija **Propiedades** y, a continuación, **Exploración de sistema** para abrir el cuadro de diálogo Propiedades de VShield.
2. Para cada módulo que desee activar, haga clic en el icono correspondiente que aparece a la izquierda del cuadro de diálogo y, a continuación, haga clic en la ficha Detección.
3. Active la casilla de verificación **Activar** que aparece en la parte superior de cada página.

Cuando lo haga, el explorador activará ese módulo. Dependiendo de la combinación de módulos que active, el icono de VShield mostrará un estado diferente.

Si activa todos los módulos, el explorador mostrará en la bandeja del sistema de Windows, a menos que desactive la casilla de verificación **Mostrar icono en la barra de tareas** en la página Detección de propiedades de exploración del sistema.

Método 4: Desde la Consola de VirusScan

Siga estos pasos:

1. Haga doble clic en el icono de la Consola de VirusScan en la bandeja del sistema Windows para llevar la ventana de la Consola al primer plano.
2. Seleccione VShield en la lista de tareas y, a continuación, elija **Activar** en el menú **Tarea**.

   La Consola activará el módulo Exploración de sistema y cualquier otro módulo previamente activado. No se puede utilizar este método para activar módulos individuales que no sean el módulo Exploración de sistema.
3. Haga clic en el botón de minimizar o de cerrar en la esquina superior derecha de la ventana de la Consola para reducirla a un icono en la bandeja del sistema.

- **NOTA:** *No* elija **Salir** en el menú **Tarea**. De esta manera se cerrará la Consola y se descargará de la memoria. Para ejecutar las tareas programadas, la Consola deberá estar activa.

Descripción de los estados de iconos en la bandeja del sistema de VShield

El explorador VShield muestra cuatro estados de icono diferentes en la bandeja del sistema de Windows para indicar los módulos que están activos, en caso de que los haya. Un módulo activo es un módulo activado por el explorador VShield o cargado en la memoria y que está listo para explorar archivos entrantes y salientes. Un módulo inactivo es un módulo desactivado por el explorador VShield. Esos módulos no exploran archivos.

La siguiente tabla muestra y describe cada estado del icono:

	Este icono significa que el explorador VShield se ha iniciado y que todos los módulos de VShield están activos
	Este icono significa que el módulo Exploración de sistema está activo, pero uno o varios de los demás módulos de VShield están inactivos
	Este icono significa que el módulo Exploración de sistema está inactivo, pero uno o varios de los demás módulos de VShield están activos
	Este icono significa que todos los módulos de VShield están inactivos

Utilización del asistente de configuración de VShield

Tras instalar el software de VirusScan y reiniciar el equipo, el explorador VShield se carga inmediatamente en la memoria y comienza a funcionar con un conjunto de opciones predeterminadas que proporcionan una protección antivirus básica. A no ser que desactive el explorador o uno de sus módulos (o lo detenga completamente), nunca tendrá que preocuparse de iniciarlo ni de programar tareas de exploración.

Sin embargo, para garantizar un nivel de seguridad más alto, deberá configurar el explorador para que funcione con el software de cliente de correo electrónico y hacer que examine minuciosamente el tráfico de Internet en busca de virus y software dañino. El asistente de configuración de VShield puede ayudarle a configurar muchas de estas opciones inmediatamente y, entonces, podrá adaptar el programa para que funcione mejor en su entorno a medida que se familiarice con el explorador y la susceptibilidad del sistema al software dañino.

Para iniciar el asistente de configuración de VShield:

1. Haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo de VShield, elija **Propiedades** y, a continuación, **Exploración de sistema** para abrir el cuadro de diálogo Propiedades de VShield.
2. Haga clic en **Asistente** situado en la esquina inferior izquierda del cuadro de diálogo para mostrar el panel de bienvenida del asistente de configuración.

Figura 4-3. Asistente de configuración de VShield: panel de bienvenida

3. Haga clic en **Siguiente>** para mostrar el panel de configuración de Exploración de sistema.

Figura 4-4. Asistente de configuración de VShield: panel Exploración de sistema

Aquí, puede indicar al explorador VShield que busque virus en los archivos con más posibilidades de estar infectados siempre que los abra, ejecute, copie, guarde o modifique de alguna forma. Entre estos archivos se incluyen varios tipos de archivos ejecutables y archivos de documentos con macros incluidas, como los archivos de Microsoft Office. El módulo Exploración de sistema explorará también los archivos almacenados en disquetes siempre que lea o escriba en ellos o cuando apague el equipo.

Cuando el módulo encuentra un virus, emite una alerta y pregunta qué medida debe aplicarse. Asimismo, el módulo registra sus acciones y resume su configuración actual en un archivo de registro que podrá consultar en cualquier momento.

4. Para activar estas funciones, haga clic en **Sí** y, a continuación, haga clic en **Siguiente>**. En caso contrario, haga clic en **No** y, a continuación, en **Siguiente>** para continuar.

   Aparecerá el panel del asistente de Exploración de correo electrónico.

Figura 4-5. Asistente de configuración de VShield: panel Exploración de correo electrónico

5. Active la casilla de verificación **Activar exploración de correo electrónico** y, a continuación, active la casilla de verificación que corresponde al tipo de cliente de correo electrónico que utiliza. Podrá elegir entre las siguientes opciones:

   - **Clientes de correo electrónico de Internet.** Active esta casilla de verificación si utiliza un cliente de correo electrónico POP-3 (Protocolo de oficina de correos) o SMTP (Protocolo simple de transferencia de correo) que envía y recibe correo estándar de Internet directamente o a través de una conexión telefónica. Si envía y recibe mensajes de correo electrónico desde casa y utiliza Netscape Mail, America Online o clientes tan utilizados como Eudora de Qualcomm o Outlook de Microsoft, asegúrese de seleccionar esta opción.

   - **Activar correo corporativo.** Active esta casilla de verificación si utiliza un sistema de correo electrónico patentado en el trabajo o en un entorno de red. La mayoría de los sistemas de este tipo utilizan un servidor de red central para recibir y distribuir los mensajes que los usuarios se envían entre sí desde las aplicaciones cliente. Estos sistema pueden enviar y recibir correo de fuera de la red o de Internet, pero normalmente lo hacen a través de una aplicación de "puerta de enlace" o gateway que se ejecuta desde el servidor.

     El módulo Exploración de correo electrónico admite los sistemas de correo electrónico corporativo que se incluyen en dos categorías generales:

     – **Lotus cc:Mail.** Seleccione este botón si utiliza cc:Mail versiones 6.x y posteriores, que emplean un protocolo patentado por Lotus para enviar y recibir correo.

– **Cliente para e-mail compatible con MAPI**. Seleccione este botón si utiliza Microsoft Exchange o Microsoft Outlook como sistema corporativo de correo electrónico.

Especifique el sistema de correo electrónico que utiliza y haga clic en **Siguiente>** para continuar.

- **NOTA:** Si usa los dos tipos de sistema de correo electrónico, active ambas casillas de verificación. No obstante, tenga en cuenta que el módulo Exploración de correo electrónico sólo admite a la vez un tipo de sistema de correo electrónico *corporativo*. Si necesita comprobar qué sistema de correo electrónico se usa en su oficina, consulte al administrador de la red.

  Asegúrese de hacer la distinción entre Microsoft Outlook y Microsoft Outlook Express. Aunque los dos programas tienen nombres similares, Outlook 97 y Outlook 98 son sistemasde correo electrónico corporativo compatibles con MAPI, mientras que Outlook Express envía y recibe el correo electrónico a través de los protocolos POP-3 y SMTP. Para obtener más información acerca de estos programas, consulte la documentación de Microsoft.

En el siguiente panel del asistente se definen las opciones para el módulo Exploración de transferencias de VShield.

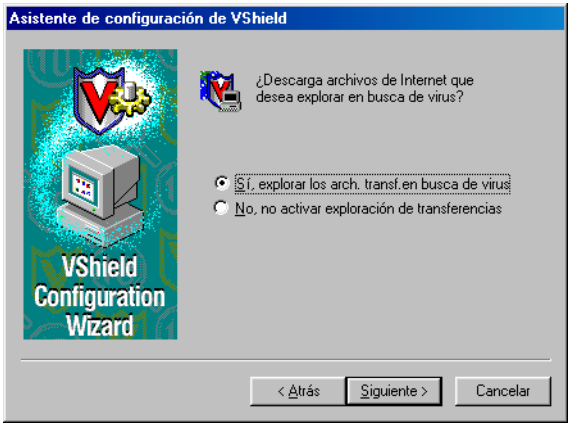

Figura 4-6. Asistente de configuración de VShield: panel Exploración de transferencias

6. Para que el módulo Exploración de transferencias busque virus en todos los archivos que descargue de Internet, active la casilla **Sí, explorar los archivos transferidos en busca de virus** y, a continuación, haga clic en **Siguiente>** para continuar.

El módulo buscará virus en los archivos con más posibilidades de infectarse y explorará los archivos comprimidos cuando los reciba.

En caso contrario, active la casilla **No, no activar exploración de transferencias** y, a continuación, haga clic en **Siguiente>** para continuar.

En el siguiente panel del asistente se definen las opciones para el módulo Filtro de Internet de VShield.

Figura 4-7. Asistente de configuración de VShield: panel Filtro de Internet

7. Para que el módulo Filtro de Internet bloquee los objetos Active X y de Java dañinos o los sitios de Internet peligrosos que pueden causar daño al sistema, seleccione **Sí, activar protección contra aplicaciones hostiles y prevención de acceso a sitios Web no seguros** y, a continuación, haga clic en **Siguiente>**.

   El módulo Filtro de Internet dispone de una lista de objetos y sitios perjudiciales que utiliza para comprobar los sitios a los que accede el usuario y los objetos que encuentra. Si alguno coincide, puede bloquearlo automáticamente u ofrecerle la opción de permitir o denegar el acceso.

   Para desactivar esta función, seleccione **No, no activar protección contra aplicaciones hostiles y prevención de acceso a sitios Web no seguros** y, a continuación, haga clic en **Siguiente>** para continuar.

   En el último panel del asistente se resumen las opciones seleccionadas.

Figura 4-8. Asistente de configuración de VShield: panel de resumen

8. Si la lista de resumen refleja con exactitud sus selecciones, haga clic en **Finalizar** para guardar los cambios y volver al cuadro de diálogo Propiedades de VShield. En caso contrario, haga clic en **<Atrás** para cambiar las opciones que seleccionó o en **Cancelar** para volver al cuadro de diálogo Propiedades de VShield sin guardar los cambios.

Definición de las propiedades del explorador VShield

Para garantizar su funcionamiento óptimo en el equipo o en el entorno de red, el explorador VShield necesita saber qué desea explorar o pasar por alto, qué debe hacer si encuentra un virus o software perjudicial y cómo debe comunicar que lo ha encontrado. Puede utilizar el asistente de configuración para activar la mayoría de las opciones de protección del explorador, pero si desea un control total sobre el funcionamiento del programa y la capacidad de adaptarlo a sus necesidades, incluyendo la capacidad de proteger la configuración con una contraseña, deberá seleccionar las opciones en el cuadro de diálogo Propiedades de VShield.

El cuadro de diálogo Propiedades de VShield consta de una serie de páginas de propiedades que controlan la configuración de cada módulo de programa. Para seleccionar las opciones, haga clic en el icono del módulo de programa que corresponda y después en cada ficha del cuadro de diálogo Propiedades de VShield de una en una.

Para abrir el cuadro de diálogo Propiedades de VShield, haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo de VShield, seleccione **Propiedades** y, a continuación, elija **Exploración de sistema**.

El cuadro de diálogo aparece con el icono de Exploración de sistema seleccionado.

Configuración del módulo Exploración de sistema

El módulo Exploración de sistema de VShield es el centro del explorador VShield. Explora los archivos de cualquier procedencia, incluyendo aquéllos que los demás módulos de VShield le envían procedentes de elementos descargados de Internet y mensajes de correo electrónico. El módulo puede comprobar si existen virus en el sistema cada vez que abre, ejecuta, copia, guarda, renombra o modifica de alguna otra manera los archivos en el disco duro, cualquier medio extraíble del equipo o unidades de red asignadas al sistema. También puede detectar virus cada vez que lee o escribe en un disquete. Como opción avanzada, se podrá activar la exploración heurística, que proporciona al explorador la capacidad de detectar virus no identificados o no clasificados.

El módulo puede realizar varias acciones automáticas para responder a los virus que encuentre y puede informar de lo que ha hecho mediante un mensaje de alerta cuando emprenda la acción o en un archivo de registro que puede revisar cuando lo crea conveniente. También puede configurarlo de modo que le pregunte lo que debe hacer cuando encuentre un virus.

En otra parte de este módulo, podrá elegir las opciones que indican al explorador VShield que muestre un icono de estado en la barra de tareas de Windows para que pueda comprobar en un instante qué módulos están activos, si los hay. Otra opción permite desactivar el módulo Exploración de sistema. Es posible que esta opción no esté disponible si ejecuta el software de VirusScan en el modo protegido.

Para seleccionar las opciones, haga clic en el icono de Exploración de sistema en el lado izquierdo del cuadro de diálogo Propiedades de exploración de sistema para ver las páginas de propiedades correspondientes a este módulo. Las siguientes secciones describen cada una de las opciones de configuración de este módulo.

Selección de las opciones de Detección

Al activarlo por primera vez, el módulo Exploración de sistema da por sentado que debe buscar virus cada vez que el usuario trabaje con cualquier archivo con posibilidades de infectarse, ya esté en el disco duro o en un disquete e independientemente de si lee o escribe el archivo en el disco duro. El módulo explorará asimismo de manera predeterminada los archivos comprimidos, pero no recurrirá a la exploración heurística a menos que esté activada.

- **NOTA:** Esta página de propiedades tendrá otro aspecto y otro conjunto de opciones dependiendo del sistema operativo utilizado en el equipo.

Para cambiar esta configuración, siga estos pasos:

1. Compruebe que esté activada la casilla de verificación **Activar exploración del sistema**.

   Al activar esta casilla de verificación, estarán disponibles las opciones restantes de esta página de propiedades. Desactive la casilla de verificación para desactivar todas las opciones de configuración de esta página e impedir que el módulo Exploración de sistema explore el sistema.

2. Indique al módulo cuándo y dónde desea que busque los virus. Puede hacer que:

   - **Explore los archivos cuando trabaje con ellos**. Cada vez que abre, ejecuta, copia, guarda, renombra o utiliza de cualquier otra forma los archivos del disco duro, el código de virus puede ejecutarse y propagar la infección a otros archivos.

     Para evitar que esto ocurra en equipos que utilizan Windows NT Workstation v4.0 ó Windows 2000 Professional, active las casillas de verificación **Archivos entrantes** y **Archivos salientes**. En los equipos que utilizan Windows 95 ó Windows 98, active las casillas de verificación **Ejecutar**, **Copiar**, **Crear** y **Renombrar** para asegurar una cobertura completa.

     Los archivos "entrantes" son archivos que el equipo u otro sistema de la red guarda o copia en discos duros locales del equipo o cualquier disco duro de red asignado al sistema. Para incluir las unidades de red asignadas al sistema para una sesión de exploración, deberá activar asimismo la casilla de verificación **Unidades de red**.

El sistema puede recibir datos procedentes de la memoria del equipo, de un disquete que está en la unidad de disquetes del equipo, de otros sistemas, de mensajes de correo electrónico o de otras fuentes y, a continuación, copiar esos datos en un archivo en el disco duro. El explorador VShield trata todos esos datos como datos "entrantes".

Los archivos "salientes", sin embargo, son archivos que el equipo u otros sistemas en la red leen en discos duros locales del sistema o unidades de red asignadas al sistema. Para incluir las unidades de red asignadas al sistema para una sesión de exploración, deberá activar asimismo la casilla de verificación **Unidades de red**.

Cuando el equipo u otro sistema lee datos de un archivo almacenado en un disco duro local del sistema o una unidad de red asignada al sistema, el módulo Exploración de sistema trata esos datos como datos "salientes".

- **NOTA:** Si tiene asignadas al equipo unidades de red de las que copia archivos o si otros usuarios de la red copian archivos de su equipo, McAfee VirusScan recomienda enérgicamente que instale el explorador VShield tanto en su equipo como en el equipo que "posee" la unidad de red. Asimismo, active todas las casillas de verificación en el área Explorar de la página Detección, además de la casilla de verificación **Unidades de red** en el área Elementos a explorar.

  Su copia del módulo Exploración de sistema comprobará entonces los archivos cuando su equipo los lea en el disco duro y también cuando los escriba en el disco duro del equipo de destino. Si el equipo de destino tiene activada su propia copia del módulo Exploración de sistema, también explorará el archivo cuando lo escriba en la unidad de red si en ese módulo está activada la casilla de verificación **Archivos entrantes**.

  Si suele copiar archivos de un servidor que no copia archivos de su equipo y si otros usuarios de la red hacen lo mismo, configure los equipos para que exploren sólo los archivos que copian en sus discos duros o sólo los archivos que leen de sus discos duros con el fin de evitar que dos equipos exploren el mismo archivo. No obstante, de hacerlo deberá configurar cada equipo de la misma manera. De lo contrario, un equipo que explora únicamente archivos salientes podría copiar un archivo infectado de un servidor que explora sólo archivos entrantes.

- **Explore los archivos de los disquetes**. Los virus de sector de arranque pueden ocultarse en los bloques de inicio de los disquetes formateados y luego cargarse en la memoria en cuanto el equipo lee datos de la unidad de disquetes. Active la casilla de verificación **Utilizar** para que el módulo Exploración de sistema compruebe los disquetes cada vez que el equipo los lee o escribe en ellos. Active la casilla de verificación **Cerrar** para que el módulo explore los disquetes que haya dejado en la unidad tras apagar el equipo. Esto garantiza que los virus no puedan cargarse cuando el equipo lea la unidad de disquetes durante el arranque.

3. Especifique los tipos de archivos que desea que examine el módulo Exploración de sistema. Podrá:

   - **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que el módulo busque virus en archivos comprimidos o en archivos de almacenamiento. Esta opción garantiza que los virus no se propaguen más allá de los archivos comprimidos. Sin embargo, como el módulo descomprime los archivos antes de explorarlos, puede que se prolongue la duración de las operaciones de exploración de un conjunto determinado de archivos mientras trabaja con el equipo.

     - **NOTA:** Cuando el módulo Exploración de sistema comprueba un archivo de almacenamiento, sólo explorará el propio archivo de almacenamiento y no los archivos comprimidos que contiene.

   - **Seleccionar los tipos de archivo que desee explorar.** Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea secuencias de comandos, macros o código binario. Por tanto, puede reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, de modo que el módulo examine únicamente los archivos con mayores posibilidades de infectarse. Para ello, seleccione el botón **Sólo archivos de programa**.

     Para ver o identificar las extensiones de nombre de archivo que debe comprobar el módulo Exploración de sistema, haga clic en **Extensiones** para abrir el cuadro de diálogo Extensiones de archivos de programa.

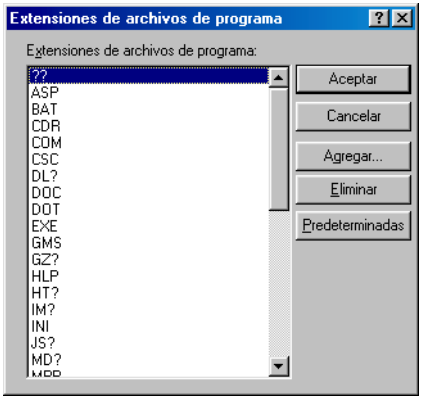

Figura 4-9. Cuadro de diálogo Extensiones de archivo de programa

- **Explorar todos los archivos.** Seleccione el botón **Todos los archivos** para que el módulo Exploración de sistema compruebe todos los archivos, independientemente de su extensión, cada vez que el usuario o un proceso del sistema los modifica de alguna manera.
- **Explorar las unidades de red.** Para que el módulo Exploración de sistema busque virus en todas las unidades asignadas al sistema, active la casilla de verificación **Unidades de red**.

- **NOTA:** Si el sistema tiene discos de red, el módulo Exploración de sistema trata todos los archivos que el sistema copia en esas unidades como archivos "entrantes" y todos los archivos que el sistema lee de esas unidades como archivos "salientes". Para garantizar una cobertura completa, active estas dos casillas de verificación en el área Explorar al activar la casilla de verificación **Unidades de red**.

---

4. Elegir las opciones de administración del software de VShield. Estas opciones permiten controlar la interacción con el explorador VShield. Podrá:

   - **Desactivar a voluntad el módulo Exploración de sistema.** Active la casilla de verificación **Exploración de sistema se puede desactivar** para tener la opción de desactivar este módulo. Tenga en cuenta que McAfee VirusScan Software recomienda dejar activado el módulo Exploración de sistema para garantizar la máxima protección. Al desactivar esta casilla de verificación, desaparecen los elementos **Salir** y **Exploración de sistema** del menú de acceso directo de VShield y el botón **Desactivar** del cuadro de diálogo Estado de VShield.

     I **SUGERENCIA:** Para asegurarse de que ningún otro usuario del equipo desactiva el explorador VShield o para reforzar la política de seguridad antivirus entre los usuarios de VirusScan en la red, desactive esta casilla de verificación y, a continuación, proteja la configuración con una contraseña. Esto impedirá que otros usuarios desactiven el explorador desde la Consola de VirusScan o desde el cuadro de diálogo Propiedades de VShield.

     También puede ejecutar todo el producto de VirusScan en modo protegido, que desactiva el acceso a todas las opciones que se pueden configurar.

   - **Mostrar el icono de VShield en la bandeja del sistema de Windows.** Active la casilla de verificación **Mostrar icono en la Barra de tareas** para que el explorador VShield muestre el icono  en la bandeja del sistema. El estado particular en el que aparece el icono depende de qué módulos de VShield estén activados.

     Al hacer doble clic en el icono se abre el cuadro de diálogo Estado de VShield. Al hacer clic con el botón derecho del ratón en el icono aparece un menú de acceso directo.

5. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración.

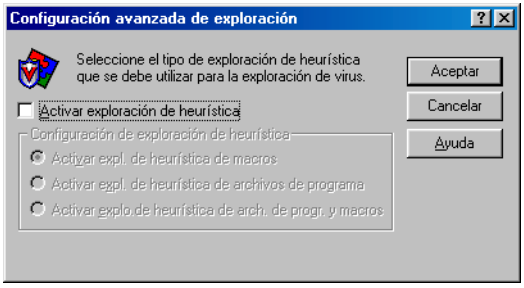

Figura 4-10. Cuadro de diálogo Configuración avanzada de exploración

La tecnología de exploración heurística permite al módulo Exploración de sistema reconocer nuevos virus basándose en su parecido a virus similares que el módulo ya conoce. Para ello, el módulo busca determinadas características "tipo virus" en los archivos especificados como objeto de la exploración. La presencia de una cantidad suficiente de estas características en un archivo lleva al módulo a identificarlo como posiblemente infectado con un virus nuevo o que aún no ha sido identificado.

Puesto que, al mismo tiempo, el módulo Exploración de sistema busca características en el archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas de infección. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

El módulo Exploración de sistema se inicia sin que esté activa ninguna opción de exploración heurística. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que desee que utilice el módulo Exploración de sistema. Podrá elegir entre las siguientes opciones:

– **Activar expl. de heurística de macros**. Seleccione esta opción para que el módulo Exploración de sistema identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que contengan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. El módulo identificará las coincidencias exactas con el nombre del virus correspondiente. Cuando las firmas de código recuerden a virus existentes, el módulo indicará que ha encontrado un posible virus de macro.

– **Activar expl. de heurística de arch. de programa.** Elija esta opción para que el módulo Exploración de sistema localice nuevos virus en archivos de programa examinando sus características y comparándolas con una lista de características de virus conocidos. El módulo identificará los archivos que tengan un número suficiente de estas características como posibles virus.

– **Activar expl. de heurística de arch. de programa y macros.** Seleccione esta opción para que el módulo utilice ambos tipos de exploración heurística. McAfee VirusScan aconseja el uso de esta opción para obtener una protección antivirus total.

• **NOTA:** El módulo Exploración de sistema utilizará técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide explorar **Todos los archivos**, el módulo utilizará la exploración heurística para todos los tipos de archivo.

c. Haga clic en **Aceptar** para guardar los cambios y volver al cuadro de diálogo Propiedades de VShield.

6. Haga clic en la ficha Acción para seleccionar otras opciones del módulo Exploración de sistema. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración del sistema, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

• **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Acción

Cuando el módulo Exploración de sistema detecta un virus, puede responder preguntando qué debe hacer con el archivo infectado o emprendiendo automáticamente la acción que se le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta debe ofrecer el módulo cuando encuentre un virus o qué acciones debe emprender automáticamente.

- **NOTA:** Esta página de propiedades tendrá otro aspecto y otro conjunto de opciones dependiendo del sistema operativo utilizado en el equipo.

Siga estos pasos:

1. Haga clic en la ficha Acción del módulo Exploración de sistema para mostrar la página de propiedades adecuada.
2. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada inmediatamente debajo de la lista cambiará para mostrar opciones adicionales para cada posible elección.

   - **NOTA:** Si selecciona **Consultar al usuario antes de realizar acción** en la lista, haga clic en la ficha Alerta para especificar si desea que el módulo Exploración de sistema avise con un mensaje, un sonido o ambos.

3. Los elementos de la lista entre los que puede elegir son:

   - **Consultar al usuario antes de realizar acción.** Elija esta respuesta para que el módulo Exploración de sistema le pregunte qué debe hacer si encuentra un virus; el programa mostrará un mensaje de alerta y le ofrecerá varias posibles respuestas.

     Si el equipo utiliza Windows 95 o Windows 98 y elige esta respuesta, aparecerá la opción Tipo de comando. Aquí, podrá elegir el método que debe utilizar el módulo Exploración de sistema para avisarle cuando encuentre un virus.

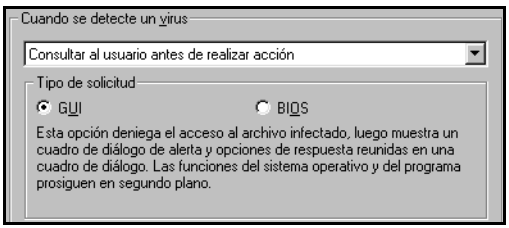

Figura 4-11. Área Tipo de comando

Podrá elegir entre las siguientes opciones:

- **BIOS.** Haga clic en este botón para ver un mensaje de alerta de pantalla completa en modo de texto que ofrece varias opciones de respuesta, incluyendo una opción que permite continuar sin emprender ninguna acción contra el virus. Este modo también detiene totalmente el sistema hasta que elija una opción de respuesta.
- **GUI.** Haga clic en este botón para ver un mensaje de alerta gráfico estándar que también ofrece varias opciones de respuesta. Entre las opciones no figura Continuar acceso. Mientras decide qué opción elegir, el sistema continuará funcionando normalmente en segundo plano.

A continuación, elija las opciones de respuesta que desee ver en ese mensaje de alerta en el área Acciones posibles situada en la parte inferior de la página de propiedades. Cada casilla de verificación que active aquí hace que aparezca un botón de opción en el mensaje de alerta que el módulo muestra cuando encuentra un virus. Por ejemplo, al seleccionar **Eliminar archivo**, aparecerá un botón u opción **Eliminar** en el mensaje de alerta. Podrá elegir entre las siguientes opciones:

- **Limpiar archivo**. Esta opción indica al módulo que intente eliminar el código de virus del archivo infectado. Si la función de elaboración de informes está activada, grabará un suceso de registro cada vez que limpie o no pueda limpiar un archivo infectado.
- **Eliminar archivo**. Esta opción indica al módulo que elimine inmediatamente el archivo infectado.
- **Mover archivo**. Esta opción indica al módulo que mueva el archivo infectado a una carpeta de cuarentena. La versión GUI de los mensajes de alerta mostrarán un botón **Mover archivo a** que permite buscar una carpeta de cuarentena.
- **Detener acceso**. Esta opción indica al módulo que impida al usuario o a cualquier otra persona que haya intentado modificar este archivo trabajar con él.
- **Excluir archivo**. Esta opción indica al módulo que ignore el archivo durante esta operación de exploración y otras posteriores.

– **Continuar acceso**. Esta opción deja intacto el archivo y en la ubicación original del equipo, y no impide al usuario abrir, copiar, renombrar o modificar de otra manera el archivo en el futuro. Utilice esta opción sólo cuando sepa con certeza que el archivo marcado por el módulo Exploración de sistema no está infectado. Para conservar los archivos como muestras de virus, McAfee VirusScan Software recomienda mover los archivos infectados a una carpeta de cuarentena.

  • **NOTA:** Esta opción está disponible únicamente en los equipos que utilizan Windows 95 o Windows 98 y únicamente cuando elige el modo **BIOS**.

- **Mover los archivos infectadosautomáticamente**. Elija esta respuesta si desea que el módulo mueva los archivos infectados a una carpeta de cuarentena tan pronto como los detecte.

  De forma predeterminada, el módulo mueve estos archivos a una carpeta denominada \Infectados ubicada en el directorio de programas de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente o hacer clic en **Examinar** para encontrar una carpeta adecuada en su disco duro.

- **Limpiar los archivos infectados automáticamente.** Elija esta respuesta para indicar al módulo que elimine el código de virus del archivo infectado tan pronto como lo detecte. Si el módulo no puede eliminar el virus, impedirá el acceso al archivo y anotará el incidente en el archivo de registro.

- **Eliminar los archivos infectados automáticamente.** Elija esta opción para que el módulo borre inmediatamente todos los archivos infectados que detecte. Asegúrese de activar la función de generación de informes para poder tener un registro de los archivos eliminados por el módulo. Tendrá que recuperar los archivos eliminados de las copias de seguridad. Si el módulo no puede eliminar un archivo infectado, anotará el incidente en el archivo de registro.

- **Impedir el acceso a los archivos infectados y continuar.** Elija esta respuesta para que el módulo marque el archivo como "prohibido" y prosiga con las operaciones normales de exploración. Elija esta respuesta únicamente si piensa dejar el equipo sin supervisión durante periodos de tiempo prolongados.

  Si también activa la función de generación de informes del módulo, el programa registrará los nombres de los virus que detecte y de los archivos infectados para que pueda eliminarlos tan pronto como tenga la oportunidad.

4. Haga clic en la ficha Alerta para seleccionar otras opciones del módulo Exploración de sistema. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración del sistema, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Alerta

Una vez configuradas las opciones de respuesta deseadas en la página Acción, el módulo Exploración de sistema puede buscar y eliminar automáticamente virus del sistema, conforme los vaya encontrando, sin casi ninguna intervención posterior. Sin embargo, si desea que el módulo le avise cuando encuentre un virus para que pueda emprender la acción apropiada, configúrelo de modo que envíe un mensaje de alerta.

Siga estos pasos:

1. Haga clic en la ficha Alerta del módulo Exploración de sistema para mostrar la página de propiedades adecuada.

2. Active la casilla de verificación **Notificar al Administrador de alertas** para que el módulo envíe mensajes de alerta al Administrador de alertas para su distribución.

   El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que el módulo Exploración de sistema envíe satisfactoriamente estos mensajes de alerta, deberá configurar también la utilidad de configuración del cliente del Administrador de alertas.

   Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

   - **NOTA:** Al desactivar esta casilla de verificación, se indica al módulo Exploración de sistema que no envíe un mensaje de alerta a través del Administrador de alertas, sin que ello afecte a otros mensajes de alerta configurados en esta página de propiedades.

3. Active la casilla de verificación **Alerta sonora** para que el módulo emita un tono cuando encuentre un archivo infectado.

Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**. El módulo hará sonar un sonido estándar de alerta del sistema o el archivo .WAV que tenga configurado el equipo.

4. Active la casilla de verificación **Mostrar mensaje personalizado** para que el módulo añada un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

   Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

5. Escriba el mensaje que debe mostrar el módulo en el cuadro de texto provisto para ello. Puede escribir 250 caracteres como máximo.

6. Haga clic en la ficha Informe para seleccionar otras opciones del módulo Exploración de sistema. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración del sistema, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Informe

El módulo Exploración de sistema enumera las opciones de configuración actuales y resume todas las acciones que emprende durante las operaciones de exploración en un archivo de registro denominado VSHLOG.TXT. Puede configurar el módulo para que escriba su registro en ese archivo o puede utilizar cualquier editor de texto para crear un archivo de texto con este fin. Después, podrá abrir e imprimir el archivo de registro para examinarlo desde cualquier editor de texto.

El archivo VSHLOG.TXT puede ser una importante herramienta de administración para realizar un seguimiento de la actividad de los virus en el sistema y tomar nota de la configuración utilizada para detectar y responder a las infecciones que encuentre el módulo Exploración de sistema. También puede utilizar los informes de incidentes que se registran en el archivo para

determinar qué archivos tiene que reemplazar a partir de las copias de seguridad, cuáles debe examinar de los que se encuentran en el área de cuarentena y cuáles debe eliminar del equipo. Utilice la página de propiedades Informe para determinar qué información debe incluir el módulo en su archivo de registro.

Para configurar el módulo Exploración de sistema de modo que anote sus acciones en un archivo de registro, siga estos pasos:

1. Haga clic en la ficha Informe del módulo Exploración de sistema para mostrar la página de propiedades adecuada.
2. Active la casilla de verificación **Registrar en archivo**.

   De manera predeterminada, el módulo Exploración de sistema escribe la información de registro en el archivo VSHLOG.TXT ubicado en el directorio de programa de VirusScan.

   Puede escribir un nombre y ruta distintos en el cuadro de texto correspondiente, o hacer clic en **Examinar** para encontrar un archivo adecuado en el disco duro o en la red. Puede utilizar otro archivo pero el archivo de texto ya debe existir. El módulo no creará un archivo nuevo.
3. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente. Si no activa esta casilla de verificación, el tamaño del archivo de registro puede aumentar hasta donde el espacio en disco o el sistema de archivos lo permita.

   Escriba un valor entre 10KB y 999KB. De manera predeterminada, el módulo Exploración de sistema limita el tamaño del archivo a 100KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, el módulo eliminará el registro existente y comenzará de nuevo desde el punto en el que se detuvo.
4. Active las casillas de verificación que correspondan a la información que desea que el módulo incluya en el archivo de registro. Normalmente, el módulo registrará los datos al término de la operación de exploración o al apagar el sistema.

   Puede elegir la información que desea registrar:

   - **Detección de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo encuentre durante cada operación de exploración. Desactive la casilla de verificación para no incluir esta información en el archivo de registro.

- **Limpieza de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de archivos infectados que el módulo limpie o intente limpiar durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Eliminación de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo elimine en cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Desplazamiento de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo mueve a una carpeta de cuarentena en cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Configuración de sesión**. Active esta casilla de verificación para que el archivo de registro incluya las opciones de configuración utilizadas para el módulo en cada sesión de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Resumen de sesión**. Active esta casilla de verificación para que el archivo de registro haga un resumen de las acciones realizadas por el módulo durante cada sesión de exploración.

  Si elige esta opción, el registro incluirá:

  – El número de archivos examinados por el módulo.

  – El número de archivos infectados limpiados por el módulo.

  – El número de archivos infectados eliminados por el módulo.

  – El número de archivos infectados trasladados por el módulo a una carpeta de cuarentena.

  – La configuración del módulo Exploración de sistema.

  Desactive la casilla de verificación para no incluir esta información en el archivo de registro.

5. **Fecha y hora**. Active esta casilla de verificación para que el archivo de registro incluya la fecha y la hora en las que el módulo comienza cada sesión de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

6. **Nombre de usuario**. Active esta casilla de verificación para que el archivo de registro incluya el nombre del usuario conectado en la estación de trabajo cuando el módulo inicie cada sesión de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

7. Haga clic en la ficha Exclusión para seleccionar otras opciones del módulo Exploración de sistema. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración del sistema, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA**: Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Exclusión

Muchos de los archivos que contiene el equipo no pueden infectarse. La comprobación de estos archivos con el módulo Exploración de sistema puede llevar mucho tiempo y generar escasos resultados. Existe la posibilidad de reducir el tiempo que el módulo Exploración de sistema dedica a la comprobación de cada archivo que se modifique limitando la exploración sólo a los tipos de archivo susceptibles de infectarse. También podrá configurar de modo que ignore los archivos o carpetas que sabe con seguridad que no pueden infectarse.

La lista de exclusión identifica los discos, carpetas o archivos individuales que desee excluir de las operaciones de exploración de VShield. De manera predeterminada, el módulo Exploración de sistema no explora la Papelera de reciclaje ya que Windows no ejecutará los elementos almacenados en dicha ubicación. Esos elementos aparecerán en la lista de exclusión la primera vez que abra la ventana.

Cada entrada en la lista de exclusión muestra la ruta de acceso al elemento, especifica si el módulo también excluirá las carpetas anidadas en el destino y explica si la aplicación excluirá el elemento al explorar los archivos, al explorar el sector de arranque del disco duro o en ambos casos.

Una vez que haya explorado exhaustivamente el sistema con el software de VirusScan, podrá configurar el módulo Exploración de sistema para que ignore aquellos archivos y carpetas que no cambian o no suelen ser vulnerables a infecciones por virus.

Para seleccionar las opciones, siga estos pasos:

1. Haga clic en la ficha Exclusión del módulo Exploración de sistema para mostrar la página de propiedades adecuada.
2. Especifique los elementos que desea excluir. Podrá:
   - **Agregar archivos, carpetas o volúmenes a la lista de exclusión.** Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar elemento de exclusión.

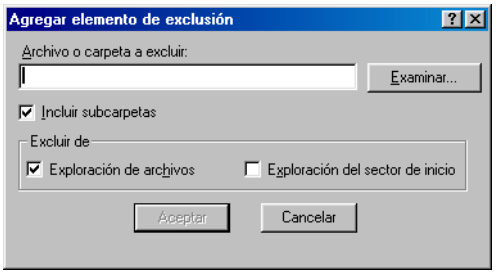

Figura 4-12. Cuadro de diálogo Agregar elemento de exclusión

A continuación, siga los siguientes pasos para agregar elementos a la lista:

a. Escriba una ruta de acceso a una carpeta o un nombre de archivo en el cuadro de texto correspondiente o haga clic en **Examinar** para buscar el elemento que el módulo deberá excluir.

   - **NOTA:** Si ha optado por trasladar los archivos infectados automáticamente a una carpeta de cuarentena, el módulo excluirá esa carpeta de las operaciones de exploración.

b. Active la casilla de verificación **Incluir subcarpetas** para indicar al módulo que ignore los archivos almacenados en cualquier subcarpeta de la carpeta especificada en el Paso a.

   - **NOTA:** Al elegir **Incluir subcarpetas**, el módulo pasará por alto sólo aquellos archivos almacenados en las propias subcarpetas. El módulo explorará los archivos almacenados en el directorio raíz de la carpeta que indique. Para excluir los archivos del directorio raíz, desactive la casilla de verificación **Incluir subcarpetas**.

c. Active la casilla de verificación **Exploración de archivos** para excluir el elemento especificado en el primer paso de las operaciones de exploración en las que el módulo busca virus que infecten archivos. Normalmente, estos virus aparecen en los archivos almacenados en los sectores visibles del disco duro.

d. Active la casilla de verificación **Exploración del sector de inicio** para excluir el elemento especificado en el primer paso de las operaciones de exploración en las que el módulo busca virus en el sector de arranque.

Estos virus normalmente aparecen en la memoria o en los archivos que residen en el sector de arranque o el registro de arranque principal del disco duro. Utilice esta opción para excluir archivos del sistema, como COMMAND.COM, de las operaciones de exploración.

+ **ADVERTENCIA:** McAfee VirusScan recomienda *no* excluir los archivos de sistema de las operaciones de exploración.

e. Repita del Paso a. al Paso d. hasta que haya incluido en la lista todos los archivos y carpetas que no desee explorar.

- **Modificar la lista de exclusión.** Para cambiar la configuración de un elemento de exclusión, selecciónelo en la lista de exclusiones y, seguidamente, haga clic en **Editar** para abrir el cuadro de diálogo Editar elemento de exclusión. Efectúe los cambios necesarios y haga clic en **Aceptar** para cerrar el cuadro de diálogo.
- **Eliminar un elemento de la lista.** Para eliminar un elemento de exclusión, selecciónelo en la lista y haga clic en **Eliminar**. Esto significa que el módulo Exploración de sistema *explorará* este archivo o esta carpeta durante la siguiente sesión de exploración.

3. Haga clic en otra ficha para modificar cualquiera de las opciones de configuración del módulo Exploración de sistema o en uno de los iconos situados en el lateral del cuadro de diálogo Propiedades de exploración del sistema para seleccionar las opciones de otro módulo.

   Para guardar los cambios del módulo Exploración de sistema sin cerrar el cuadro de diálogo, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Configuración del módulo Exploración de correo electrónico

El módulo Exploración de correo electrónico de VShield busca virus en los archivos adjuntos a mensajes de correo electrónico recibidos a través de los sistemas corporativos de correo electrónico que cumplen con el estándar MAPI (Interfaz de programación de aplicaciones de mensajería), tales como Microsoft Exchange y Outlook o versiones posteriores de Lotus cc:Mail. Incluye asimismo un modo de exploración especial que busca virus en las versiones anteriores de cc:Mail.

Este módulo puede funcionar conjuntamente con el módulo Exploración de transferencias para examinar los mensajes que llegan a través de los programas cliente de correo electrónico POP3 ó SMTP, como Eudora, Netscape Mail u Outlook Express. El módulo presta especial atención a los archivos adjuntos que llegan con el correo electrónico y que son las principales fuentes potenciales de virus. Ya que puede explorar los mensajes de correo electrónico en el momento en que aparecen en el escritorio, el módulo intercepta los virus sin darles la oportunidad de propagarse.

Al encontrar un virus, el módulo puede preguntarle qué debe hacer, o emprender automáticamente varias acciones de respuesta. Puede configurarlo para que informe de lo que ha hecho mediante un mensaje de alerta cuando emprende la acción o en un archivo de registro que puede revisar cuando lo crea conveniente. Incluso puede enviar un mensaje a la persona que envió el mensaje de correo electrónico infectado, lo cual facilita bastante el seguimiento del origen de las infecciones por virus.

- **NOTA:** El módulo Exploración de correo electrónico no aparecerá en el cuadro de diálogo Propiedades de VShield a menos que se haya utilizado la opción de instalación personalizada al instalar el software de VirusScan y al especificar que se desea utilizar el módulo Exploración de correo electrónico.

  De manera predeterminada, el explorador VShield *no* activa el módulo Exploración de correo electrónico cuando se inicia por primera vez; se ha de indicar al módulo qué sistemas de correo electrónico se utilizan antes de que pueda activarse.

Selección de las opciones de Detección

El explorador VShield no se inicia con el módulo Exploración de correo electrónico activado de manera predeterminada ya que necesita saber qué sistema de correo electrónico se utiliza. Tras configurarlo para el cliente de correo electrónico habitual, el módulo utilizará su perfil MAPI o su nombre de usuario y contraseña de cc:Mail para entrar en la cuenta de correo cuando inicie una operación de exploración.

Si ya ha iniciado y entrado en el sistema de correo electrónico, el módulo trabajará simplemente dentro de la operación de exploración que ha creado. Sin embargo, si aún no ha entrado en el sistema de correo electrónico, el módulo le pedirá que seleccione un perfil o introduzca información sobre la cuenta cuando inicie una operación de exploración, incluso antes de que haya entrado en su cuenta de correo electrónico. Esto también puede suceder al iniciar el equipo si no ha configurado el programa cliente de correo electrónico para que se cargue al inicio.

Si cambia los perfiles o entra en otra cuenta, quizás en otro dominio, el módulo pedirá que seleccione el perfil que desee utilizar o facilite un nuevo nombre de usuario y contraseña para entrar en el sistema de correo.

Para seleccionar las opciones de configuración de esta página, siga estos pasos:

1. Seleccione la casilla de verificación **Activar exploración de archivos adjuntos de correo electrónico**.

   Se activarán las demás opciones de la página de propiedades.

2. Seleccione el tipo de sistema de correo electrónico que utiliza. Las opciones disponibles son:

   - **Activar correo corporativo.** Active esta casilla de verificación para que el módulo Exploración de correo electrónico examine los archivos adjuntos al correo electrónico que se reciben a través de un sistema de correo que se ejecuta dentro de la red de la oficina. Normalmente, los sistemas de este tipo utilizan un protocolo de correo exclusivo y tienen un servidor de correo central al que se envía el correo para su distribución. Con frecuencia, estos sistemas envían y reciben correo de Internet, pero suelen hacerlo a través de una aplicación de "puerta de enlace" o gateway. El módulo Exploración de correo electrónico admite dos tipos de sistemas de correo corporativo:

     – **Microsoft Exchange (MAPI).** Seleccione este botón si utiliza un sistema de correo electrónico que envía y recibe mensajes a través de la interfaz de programación de aplicaciones de mensajería de Microsoft (MAPI), un protocolo de correo de Windows. Algunos ejemplos son: Microsoft Exchange, Microsoft Outlook 97 y Outlook 98.

– **Lotus cc:Mail.** Seleccione este botón si utiliza cc:Mail 6.x o 7.x. Estos sistemas utilizan un protocolo patentado por Lotus para enviar y recibir correo electrónico. También puede instalar cc:Mail versión 8.0 o posterior de modo que utilice el mismo protocolo que las versiones anteriores de cc:Mail. Para averiguar qué sistema utiliza, póngase en contacto con el administrador de la red.

• **NOTA:** Sólo puede seleccionar un sistema de correo *corporativo* a la vez, pero puede configurar el módulo Exploración de correo electrónico para que explore todos los archivos adjuntos que llegan a través de sistemas de correo corporativo e Internet, si utiliza los dos.

• **Correo de Internet (requiere exploración de archivos transferidos).** Active esta casilla de verificación para que el módulo Exploración de correo electrónico explore los archivos adjuntos al correo de Internet que envía y recibe mediante el Protocolo de oficina de correos (POP-3) o el Protocolo simple de transferencia de correo (SMTP). Elija esta opción si trabaja desde casa o a través de un proveedor de servicios de Internet con software como Eudora Pro de Qualcomm, Outlook Express de Microsoft o Netscape Mail.

E **IMPORTANTE:** Como el correo de Internet y los demás archivos que descarga desde los sitios Web u otras fuentes se reciben a través del mismo “canal”, el módulo Exploración de correo electrónico utiliza las opciones de detección, acción, alerta y generación de informes que se configuran en el módulo Exploración de transferencias para determinar el modo de respuesta al correo entrante de Internet. Por lo tanto, para explorar los archivos adjuntos al correo de Internet, deberá activar el módulo Exploración de transferencias y utilizar sus páginas de propiedades para seleccionar la configuración que desee.

---

3. Indique al módulo Exploración de correo electrónico qué fuentes de correo debe controlar:

   • Si elige **Microsoft Exchange (MAPI)** como sistema corporativo de correo electrónico, el área Carpetas muestra **Todo el correo entrante**, que significa que el módulo buscará virus en los archivos adjuntos a cada mensaje de correo electrónico en cuanto llegue al buzón MAPI o a través de otros servicios MAPI.

   • Si elige **Lotus cc:Mail** como sistema corporativo de correo electrónico, deberá indicar al módulo la frecuencia con la que debe explorar el buzón de entrada de cc:Mail.

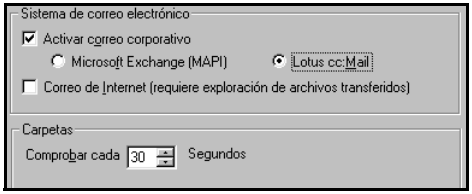

Figura 4-13. Página Detección con la opción de cc:Mail seleccionada

En el área Carpetas, introduzca el número de segundos que el módulo Exploración de correo electrónico deberá esperar antes de comprobar si hay correo nuevo en el buzón de entrada de cc:Mail. De manera predeterminada, el módulo lo comprueba cada minuto. Asegúrese de establecer un intervalo menor que el establecido para recibir los mensajes de correo electrónico de modo que el módulo pueda detectar los virus antes de que lleguen al equipo.

4. Especifique los tipos de archivos adjuntos al correo electrónico que deberá examinar el módulo Exploración de correo electrónico. Podrá:

   - **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que el módulo busque virus en archivos comprimidos o en archivos de almacenamiento. Esta opción garantiza que los virus no se propaguen más allá de los archivos comprimidos. Sin embargo, como el módulo descomprime los archivos antes de explorarlos, puede que se prolongue la duración de las operaciones de exploración de un conjunto determinado de archivos mientras trabaja con el equipo.

     - **NOTA:** Cuando el módulo Exploración de correo electrónico comprueba un archivo de almacenamiento, sólo explorará el propio archivo de almacenamiento y no los archivos comprimidos que contiene.

   - **Seleccionar los tipos de archivo que desee explorar.** Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea secuencias de comandos, macros o código binario. Por tanto, puede reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, de modo que el módulo examine únicamente los archivos con mayores posibilidades de infectarse. Para ello, seleccione el botón **Sólo archivos de programa**.

Para ver o identificar las extensiones de nombre de archivo que va a explorar el módulo Exploración de correo electrónico, haga clic en **Extensiones** para abrir el cuadro de diálogo Extensiones de archivos de programa.

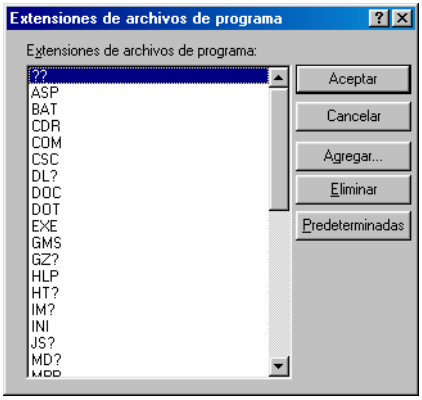

Figura 4-14. Cuadro de diálogo Extensiones de archivos de programa

- **Explorar todos los archivos.** Seleccione el botón **Todos los archivos** para que el módulo Exploración de correo electrónico compruebe todos los archivos, independientemente de su extensión, cada vez que el usuario o un proceso del sistema los modifica de alguna manera.

5. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración.

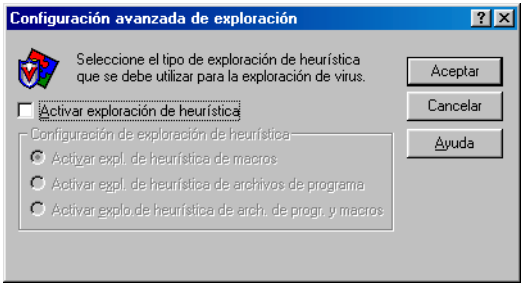

Figura 4-15. Cuadro de diálogo Configuración avanzada de exploración

La tecnología de exploración heurística permite al módulo Exploración de correo electrónico reconocer nuevos virus basándose en el parecido a virus similares que el módulo ya conoce.

Para ello, el módulo busca determinadas características "tipo virus" en los archivos especificados como objeto de la exploración. La presencia de una cantidad suficiente de estas características en un archivo lleva al módulo a identificarlo como posiblemente infectado con un virus nuevo o que aún no ha sido identificado.

Como el módulo Exploración de correo electrónico busca simultáneamente características de archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

El módulo Exploración de correo electrónico se inicia sin las opciones de exploración heurística activas. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que desee que utilice el módulo Exploración de correo electrónico. Podrá elegir entre las siguientes opciones:

   – **Activar expl. de heurística de macros**. Seleccione esta opción para que el módulo Exploración de correo electrónico identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que incluyan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. El módulo identificará las coincidencias exactas con el nombre del virus correspondiente. Cuando las firmas de código recuerden a virus existentes, el módulo indicará que ha encontrado un posible virus de macro.

   – **Activar expl. de heurística de arch. de programa.** Seleccione esta opción para que el módulo Exploración de correo electrónico localice nuevos virus en archivos de programa examinando las características de los archivos y comparándolas con una lista de características de virus conocidas. El módulo identificará los archivos que tengan un número suficiente de estas características como posibles virus.

   – **Activar expl. de heurística de arch. de programa y macros.** Seleccione esta opción para que el módulo utilice ambos tipos de exploración heurística. McAfee VirusScan Software aconseja el uso de esta opción para obtener una protección antivirus total.

- **NOTA:** El módulo utilizará técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide explorar **Todos los archivos**, el módulo utilizará la exploración heurística para todos los tipos de archivo.

6. Haga clic en la ficha Acción para seleccionar otras opciones del módulo Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Acción

Cuando el módulo Exploración de correo electrónico detecta un virus en un archivo adjunto a un mensaje de correo, puede responder preguntando qué debe hacer con el archivo infectado o emprendiendo automáticamente la acción que le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta debe ofrecer el módulo cuando encuentre un virus o qué acciones debe emprender automáticamente.

- **NOTA:** El módulo Exploración de correo electrónico puede responder a los virus sólo cuando debe explorar un sistema corporativo de correo electrónico. Si sólo selecciona Correo de Internet, las opciones no estarán disponibles. Si sólo recibe correo de Internet, deberá seleccionar las respuestas en la página de propiedades Acción del módulo Exploración de transferencias.

Siga estos pasos:

1. Haga clic en la ficha Acción del módulo Exploración de correo electrónico para mostrar la página de propiedades adecuada.
2. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada debajo de la lista cambiará para mostrar opciones adicionales para cada respuesta. Podrá elegir entre las siguientes opciones:
   - **Consultar al usuario antes de realizar acción.** Elija esta respuesta para que el módulo Exploración del correo electrónico le pregunte qué debe hacer si encuentra un virus; el programa mostrará un mensaje de alerta y le ofrecerá varias posibles respuestas.

- **NOTA:** Si elige **Consultar al usuario antes de realizar acción** en la lista, haga clic en la ficha Alerta para especificar si desea que el módulo Exploración de correo electrónico envíe un mensaje, emita una señal sonora o realice ambas acciones.

Seleccione las opciones que desee ver en el mensaje de alerta. Cada casilla de verificación que se active en esta página hace que aparezca un botón en el mensaje de alerta que el módulo muestra al encontrar un virus. Por ejemplo, al seleccionar **Eliminar archivo**, aparecerá un botón **Eliminar** en el mensaje de alerta.

Puede seleccionar una de las siguientes opciones:

– **Limpiar archivo**. Esta opción indica al módulo que intente eliminar el código de virus del archivo infectado. Si la función de elaboración de informes está activada, grabará un suceso de registro cada vez que limpie o no pueda limpiar un archivo infectado.

  - **NOTA:** El módulo Exploración de correo electrónico *no* admite esta opción para los sistemas de correo electrónico Lotus cc:Mail v7.x y anteriores. La opción no aparecerá aquí si se ha seleccionado Lotus cc:Mail en la página Detección del módulo Exploración de correo electrónico.

– **Eliminar archivo**. Esta opción indica al módulo que elimine inmediatamente el archivo adjunto infectado. Sin embargo, el módulo conservará el mensaje de correo electrónico en el que llegó.

– **Mover archivo**. Esta opción indica al módulo que mueva el archivo infectado a una carpeta de cuarentena. Los mensajes de alerta mostrarán un botón **Mover archivo a** que permite al usuario buscar una carpeta de cuarentena.

– **Continuar la exploración.** Esta opción indica al módulo que continúe la exploración sin emprender ninguna otra acción. Si las opciones de generación de informes están activadas, el módulo incluirá el incidente en su archivo de registro.

- **Mover archivos infectados a una carpeta**. Elija esta respuesta si desea que el módulo mueva los archivos infectados a una carpeta de cuarentena tan pronto como los detecte. El módulo mueve estos archivos a una carpeta denominada Infectados ubicada en el directorio de programa de VirusScan.

Puede cambiar el nombre y ubicación de la carpeta en la que el módulo guarda el correo de Internet infectado pero, para ello, deberá pasar al módulo Exploración de transferencias y hacer clic en la ficha Acción.

- **Limpiar archivos infectados**. Elija esta respuesta para indicar al módulo que elimine el código de virus del archivo infectado tan pronto como lo detecte. Si el módulo no puede eliminar el virus, anotará el incidente en el archivo de registro.

  - **NOTA:** El módulo Exploración de correo electrónico *no* admite esta opción para los sistemas de correo electrónico Lotus cc:Mail v7.x y anteriores. La opción no aparecerá aquí si se ha seleccionado Lotus cc:Mail en la página Detección del módulo Exploración de correo electrónico.

- **Eliminar archivos infectados.** Elija esta respuesta para que el módulo Exploración de correo electrónico elimine inmediatamente todos los archivos infectados que detecte. Asegúrese de activar la función de generación de informes para poder tener un registro de todos los archivos eliminados por el módulo. Tendrá que recuperar los archivos eliminados de las copias de seguridad.

- **Continuar la exploración.** Elija esta respuesta para que el módulo continúe la exploración sin emprender acción alguna contra los virus que detecta. Si también activa la función de generación de informes de Exploración de correo electrónico, el programa registrará los nombres de los virus que detecte y de los archivos infectados para que pueda eliminarlos tan pronto como tenga la oportunidad.

  Utilice esta opción sólo si tiene pensado dejar el equipo sin supervisión mientras el módulo comprueba si hay virus.

3. Haga clic en la ficha Alerta para seleccionar otras opciones del módulo Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Alerta

Una vez configuradas las opciones de respuesta deseadas en la página Acción, el módulo Exploración de correo electrónico puede buscar y eliminar automáticamente los virus del sistema, conforme los vaya encontrando, sin casi ninguna intervención posterior. Sin embargo, si desea que el módulo le advierta cuando encuentra un virus para que pueda emprender la acción apropiada, configúrelo de modo que envíe un mensaje de alerta.

Siga estos pasos:

1. Haga clic en la ficha Alerta del módulo Exploración de correo electrónico para mostrar la página de propiedades adecuada.
2. Active la casilla de verificación **Notificar al Administrador de alertas** para que el módulo envíe mensajes de alerta al Administrador de alertas para su distribución.

   El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que el módulo Exploración de correo electrónico envíe satisfactoriamente estos mensajes de alerta, deberá configurar también la utilidad de configuración del cliente del Administrador de alertas.

   Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

   - **NOTA:** Si desactiva esta casilla de verificación, indicará al módulo Exploración de correo electrónico que no envíe un mensaje de alerta a través del Administrador de alertas, sin que ello afecte a otros mensajes de alerta configurados en esta página de propiedades.

   Como parte del sistema de avisos antivirus, el módulo Exploración de correo electrónico puede responder directamente con un mensaje de alerta a cualquier persona que le envíe un mensaje o un archivo adjunto infectado. Puede copiar ese mensaje y enviarlo a otros destinatarios, dentro y fuera de su empresa. Si prefiere no enviar una respuesta, podrá simplemente configurar el módulo para que envíe una notificación de correo electrónico, quizás a un administrador del sistema, cada vez que detecte un virus.

El envío de mensajes de respuesta podrá servir para detectar las fuentes de los virus y determinar por dónde se introducen los agentes infecciosos en la red. El envío de copias de estos mensajes a los administradores del sistema puede ayudarles a realizar un seguimiento de la propagación de las infecciones.

También puede optar por enviar mensajes a cualquier destinatario sin responder al emisor del archivo adjunto infectado. El módulo Exploración de correo electrónico puede obtener los destinatarios directamente de la libreta de direcciones de Microsoft Exchange, Microsoft Outlook, de otras compatibles con MAPI o de cualquier directorio Lotus cc:Mail equivalente. También puede introducir directamente las direcciones de los destinatarios.

El mensaje que cree para las respuestas es una plantilla. El módulo Exploración de correo electrónico enviará ese mensaje automáticamente a cada destinatario que designe, por lo que McAfee VirusScan Software recomienda escribir un mensaje que todos los destinatarios puedan leer y entender. Aparte de los pasos que debe emprender para escribir el mensaje de la plantilla, el módulo no le dará la oportunidad de modificar el mensaje antes de enviarlo.

Puede enviar un mensaje para responder al emisor del mensaje infectado y otro diferente al resto de destinatarios, pero no podrá adaptar el mismo mensaje para distintos destinatarios.

3. Para elaborar los mensajes de plantilla, siga los siguientes pasos:

   a. Active la casilla de verificación **Responder correo a remitente** en la página de propiedades Alerta y, a continuación, haga clic en **Configurar** para abrir un formulario de mensaje de correo estándar.

      Como el módulo devolverá este mensaje directamente al emisor del mensaje de correo electrónico infectado, el botón **Para:** y el cuadro de texto no estarán disponibles.

   b. Para enviar una copia de este mensaje a otra persona, escriba su dirección de correo electrónico en el cuadro de texto Cc:, o bien haga clic en **Cc:** para elegir un destinatario en la libreta de direcciones o el directorio del usuario del sistema de correo electrónico.

- **NOTA:** Para buscar una dirección de correo electrónico en el directorio del usuario del sistema de correo electrónico, deberá almacenar la información con las direcciones en un directorio del usuario, base de datos o libreta de direcciones compatibles con MAPI, o bien en un directorio Lotus cc:Mail equivalente. Si aún no ha entrado en el sistema de correo electrónico, el módulo Exploración de correo electrónico tratará de utilizar el perfil MAPI predeterminado para entrar en los sistemas de correo compatibles con MAPI o le solicitará el nombre de usuario, la contraseña y la ruta de acceso al buzón de Lotus cc:Mail. Introduzca la información que el módulo necesita y, a continuación, haga clic en **Aceptar** para continuar.

c. Especifique un asunto en el mensaje que refleje la importancia del mismo y agregue algún comentario en el cuerpo del mensaje, debajo de una notificación de virus estándar que facilitará el propio módulo. Puede añadir hasta 1.024 caracteres de texto.

d. Haga clic en **Aceptar** para guardar el mensaje.

Siempre que detecte un virus, el módulo enviará una copia de este mensaje a todas las personas que le envíen un correo electrónico con un archivo adjunto infectado. El programa tomará la dirección del destinatario de la información encontrada en la cabecera del mensaje original e identificará el virus y el archivo afectado en el área que se encuentra justo debajo de la línea de asunto. Si tiene activada la función de generación de informes, el módulo también registrará cada incidente cuando envíe un mensaje de alerta.

e. Para enviar un mensaje de correo electrónico con el fin de advertir a otros usuarios de un archivo adjunto infectado, por ejemplo, a un administrador de red, active la casilla de verificación **Enviar correo de alerta a usuario** en la página de propiedades Alerta. Podrá escribir una respuesta estándar del mismo modo que lo hizo desde el Paso a al Paso d. Sin embargo, en este caso podrá rellenar los cuadros de texto Para: y Cc:.

Siempre que detecte un virus, el módulo Exploración de correo electrónico enviará una copia de este mensaje a todas las direcciones que escriba para el mismo.

4. Active la casilla de verificación **Alerta sonora** para que el módulo emita un tono cuando encuentre un archivo infectado.

Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**.

El módulo hará sonar un sonido estándar de alerta del sistema o el archivo .WAV que tenga configurado el equipo.

5. Active la casilla de verificación **Mostrar mensaje personalizado** para que el módulo añada un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

   Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

6. Escriba el mensaje que debe mostrar el módulo en el cuadro de texto provisto para ello. Puede escribir 250 caracteres como máximo.

7. Haga clic en la ficha Informe para seleccionar otras opciones del módulo Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Informe

El módulo Exploración de correo electrónico enumera las opciones de configuración actuales y resume todas las acciones que emprende durante las operaciones de exploración en un archivo de registro denominado WEBEMAIL.TXT. Puede configurar el módulo para que escriba su registro en ese archivo o puede utilizar cualquier editor de texto para crear un archivo de texto con este fin. Después, podrá abrir e imprimir el archivo de registro para examinarlo desde cualquier editor de texto.

El archivo WEBEMAIL.TXT puede ser una importante herramienta de administración para realizar un seguimiento de la actividad de los virus en el sistema y tomar nota de las opciones de configuración utilizadas para detectar y responder a las infecciones encontradas por el módulo. También puede utilizar los informes de incidentes que se registran en el archivo para determinar qué archivos tiene que reemplazar a partir de las copias de seguridad, cuáles debe examinar de los que se encuentran en el área de cuarentena y cuáles debe eliminar del equipo. Utilice la página de propiedades Informe para determinar qué información debe incluir el módulo en su archivo de registro.

Para configurar el módulo Exploración de correo electrónico de modo que anote sus acciones en un archivo de registro, siga estos pasos:

1. Haga clic en la ficha Informe del módulo Exploración de correo electrónico para mostrar la página de propiedades adecuada.
2. Active la casilla de verificación **Registrar en archivo**.

   Como opción predeterminada, el módulo escribe la información de registro en el archivo WEBEMAIL.TXT del directorio de programa de VirusScan. Puede introducir un nombre y una ruta de acceso distintos en el cuadro de texto correspondiente o hacer clic en **Examinar** para buscar un archivo idóneo en el disco duro o en la red.
3. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente. Si no activa esta casilla de verificación, el tamaño del archivo de registro puede aumentar hasta donde el espacio en disco o el sistema de archivos lo permita.

   Escriba un valor entre 10 KB y 999 KB. De manera predeterminada, el módulo Exploración de sistema limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, el módulo eliminará el registro existente y comenzará de nuevo desde el punto en el que se detuvo.
4. Active las casillas de verificación que correspondan a la información que desea que el módulo incluya en el archivo de registro. Normalmente, el módulo registrará los datos al término de la operación de exploración o al apagar el sistema.

Puede decidir que se registre la siguiente información:

- **Detección de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo encuentre durante cada operación de exploración. Desactive la casilla de verificación para no incluir esta información en el archivo de registro.
- **Eliminación de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo elimine en cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información.
- **Desplazamiento de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo mueve a una carpeta de cuarentena en cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información.
- **Configuración de sesión**. Active esta casilla de verificación para que el archivo de registro incluya las opciones de configuración utilizadas para el módulo en cada sesión de exploración. Desactive esta casilla de verificación para no incluir esta información.
- **Resumen de sesión**. Active esta casilla de verificación para que el archivo de registro haga un resumen de las acciones realizadas por el módulo durante cada sesión de exploración. El registro incluirá:
  - El número de archivos examinados por el módulo.
  - El número de archivos infectados limpiados por el módulo (sólo sistemas de correo electrónico MAPI).
  - El número de archivos infectados eliminados por el módulo.
  - El número de archivos infectados trasladados por el módulo a una carpeta de cuarentena.
  - La configuración del módulo Exploración de correo electrónico.

  Desactive la casilla de verificación para no incluir esta información.
- **Limpieza de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de archivos infectados que el módulo limpie o intente limpiar durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información.

- **NOTA:** El módulo Exploración de correo electrónico *no* admite esta opción para los sistemas de correo electrónico Lotus cc:Mail v7.x y anteriores. La opción no aparecerá aquí si se ha seleccionado Lotus cc:Mail en la página Detección del módulo Exploración de correo electrónico.

5. Haga clic en otra ficha para modificar cualquiera de las opciones de configuración de Exploración de correo electrónico o en uno de los iconos situados en el lateral del cuadro de diálogo de propiedades de exploración del correo electrónico para seleccionar opciones de otro módulo.

   Para guardar los cambios del módulo Exploración de correo electrónico sin cerrar el cuadro de diálogo, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Configuración del módulo Exploración de transferencias

El módulo Exploración de descargas puede comprobar los archivos descargados de Internet cuando se visitan sitios Web, sitios FTP y otros sitios de Internet. Es en este módulo donde también se configuran las opciones que se desean utilizar para responder a los archivos adjuntos al correo electrónico infectados que se reciben a través de programas cliente de correo electrónico POP-3 o SMTP como Eudora, Netscape Mail o Microsoft Outlook Express. Para activar esta función, deberá elegir un sistema de correo adecuado en la página Detección del módulo Exploración de correo electrónico.

Al encontrar un virus, el módulo puede preguntarle qué debe hacer, o emprender automáticamente varias acciones de respuesta. Puede configurarlo para que informe de lo que ha hecho mediante un mensaje de alerta cuando emprende la acción o en un archivo de registro que puede revisar cuando lo crea conveniente. Incluso puede enviar un mensaje a la persona que envió el mensaje de correo electrónico infectado, lo cual facilita bastante el seguimiento del origen de las infecciones por virus.

- **NOTA:** El módulo Exploración de transferencias *no* aparecerá en el cuadro de diálogo Propiedades de VShield a menos que se haya utilizado la opción de instalación personalizada al instalar el software de VirusScan y se haya optado por la instalación del componente de exploración de Internet.

Selección de las opciones de Detección

En principio, el módulo Explorador de transferencias da por supuesto que el usuario desea buscar virus cada vez que descarga de Internet un archivo con posibilidades de infectarse. Estas opciones predeterminadas proporcionan una protección excelente, pero su entorno podría precisar una configuración diferente.

Para modificar las opciones de esta página de propiedades, siga estos pasos:

1. Active la casilla de verificación **Activar exploración de descarga de Internet**.

   Se activarán las demás opciones de la página de propiedades.

2. Especifique los tipos de archivo que deberá examinar el módulo Exploración de transferencias. Podrá:

   - **Seleccionar los tipos de archivo que desee explorar.** Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea secuencias de comandos, macros o código binario. Por tanto, puede reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, de modo que el módulo examine únicamente los archivos con mayores posibilidades de infectarse. Para ello, seleccione el botón **Sólo archivos de programa**.

     Para ver o designar las extensiones de nombre de archivo que va a examinar el módulo Exploración de transferencias, haga clic en **Extensiones** para abrir el cuadro de diálogo Extensiones de archivos de programa.

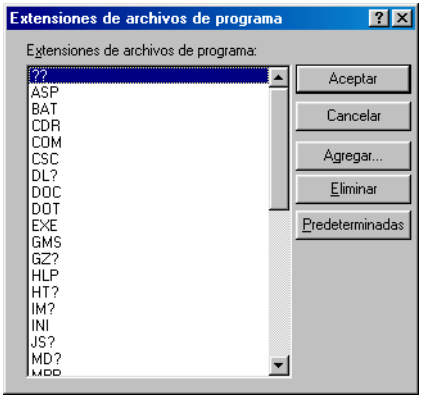

Figura 4-16. Cuadro de diálogo Extensiones de archivos de programa

- **Explorar todos los archivos.** Seleccione el botón **Todos los archivos** para que el módulo Exploración de transferencias examine todos los archivos, independientemente de su extensión, cada vez que el usuario o un proceso de sistema los modifique de alguna manera.
- **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que el módulo busque virus en archivos comprimidos o en archivos de almacenamiento.

  Esta opción garantiza que los virus no se propaguen más allá de los archivos comprimidos. Sin embargo, como el módulo descomprime los archivos antes de explorarlos, puede que se prolongue la duración de las operaciones de exploración de un conjunto determinado de archivos mientras trabaja con el equipo.

- **NOTA:** Cuando el módulo Exploración de transferencias examina un archivo de almacenamiento, sólo explora el propio archivo de almacenamiento y no los archivos comprimidos que contiene.

---

3. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración.

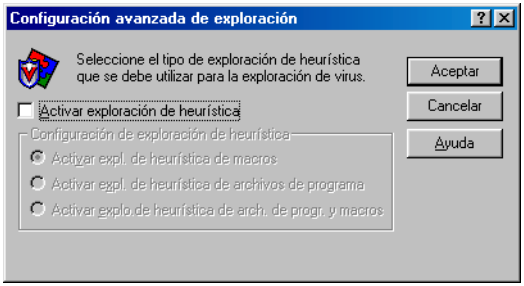

Figura 4-17. Cuadro de diálogo Configuración avanzada de exploración

La tecnología de exploración heurística permite al módulo Explorador de transferencias reconocer nuevos virus basándose en su parecido a otros virus similares que el módulo ya conoce. Para ello, el módulo busca determinadas características "tipo virus" en los archivos especificados como objeto de la exploración. La presencia de una cantidad suficiente de estas características en un archivo lleva al módulo a identificarlo como posiblemente infectado con un virus nuevo o que aún no ha sido identificado.

Como el módulo Exploración de transferencias busca simultáneamente características de archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas acerca de infecciones de virus. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

El módulo Explorador de elementos descargados se inicia sin ninguna opción de exploración heurística activa. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que deberá utilizar el módulo Exploración de transferencias. Podrá elegir entre las siguientes opciones:

   – **Activar expl. de heurística de macros**. Seleccione esta opción para que el módulo Exploración de transferencias identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que incluyan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. El módulo identificará las coincidencias exactas con el nombre del virus correspondiente. Cuando las firmas de código recuerden a virus existentes, el módulo indicará que ha encontrado un posible virus de macro.

   – **Activar expl. de heurística de arch. de programa.** Elija esta opción para que el módulo Exploración de transferencias localice nuevos virus en archivos de programa examinando sus características y comparándolas con una lista de características de virus conocidos. El módulo identificará los archivos que tengan un número suficiente de estas características como posibles virus.

   – **Activar expl. de heurística de arch. de programa y macros.** Seleccione esta opción para que el módulo utilice ambos tipos de exploración heurística. McAfee VirusScan Software aconseja el uso de esta opción para obtener una protección antivirus total.

- **NOTA:** El módulo Exploración de transferencias utilizará las técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide explorar **Todos los archivos**, el módulo utilizará la exploración heurística para todos los tipos de archivo.

c. Haga clic en **Aceptar** para guardar la configuración y volver al cuadro de diálogo Propiedades de VShield.

4. Haga clic en la ficha Acción para seleccionar otras opciones del módulo Exploración de transferencias. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración de descarga, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Acción

Cuando el módulo Exploración de transferencias detecta un virus, puede responder preguntando qué debe hacer con el archivo infectado o emprendiendo automáticamente la acción que se le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta debe ofrecer el módulo cuando encuentre un virus o qué acciones debe emprender automáticamente.

Siga estos pasos:

1. Haga clic en la ficha Acción del módulo Exploración de transferencias para mostrar la página de propiedades adecuada.
2. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada inmediatamente debajo de la lista cambiará para mostrar opciones adicionales para cada posible elección. Podrá elegir entre las siguientes opciones:
   - **Consultar al usuario antes de realizar acción.** Elija esta respuesta para que el módulo Explorador de elementos descargados le pregunte qué debe hacer si encuentra un virus; el programa mostrará un mensaje de alerta y le ofrecerá varias posibles respuestas.

- **NOTA:** Si selecciona **Consultar al usuario antes de realizar acción** en la lista, haga clic en la ficha Acción para especificar si el módulo Exploración de transferencias debe advertirle mediante un mensaje, una señal sonora o ambas acciones.

Seleccione las opciones que desee ver en el mensaje de alerta. Cada casilla de verificación que se active en esta página hace que aparezca un botón en el mensaje de alerta que el módulo muestra al encontrar un virus. Por ejemplo, al seleccionar **Eliminar archivo**, aparecerá un botón **Eliminar** en el mensaje de alerta.

Puede seleccionar una de las siguientes opciones:

- **Eliminar archivo**. Esta opción indica al módulo que elimine inmediatamente el archivo adjunto infectado. Sin embargo, el módulo conservará el mensaje de correo electrónico en el que llegó.
- **Mover archivo**. Esta opción indica al módulo que mueva el archivo infectado a una carpeta de cuarentena. El mensaje de alerta mostrará un botón **Mover** que indica al módulo que mueva el archivo infectado a un directorio de cuarentena previamente seleccionado. De manera predeterminada, este directorio es una carpeta denominada Infectados en el directorio de programa de VirusScan.
- **Continuar la exploración.** Esta opción indica al módulo que continúe con la exploración sin emprender ninguna otra acción. Si las opciones de generación de informes están activadas, el módulo incluirá el incidente en su archivo de registro.

- **Mover archivos infectados a una carpeta**. Elija esta respuesta si desea que el módulo mueva los archivos infectados a una carpeta de cuarentena tan pronto como los detecte. El módulo mueve estos archivos a una carpeta denominada Infectados ubicada en el directorio de programa de VirusScan.
- **Eliminar archivos infectados.** Elija esta respuesta para que el módulo Explorador de transferencias elimine inmediatamente todos los archivos infectados que detecte. Asegúrese de activar la función de generación de informes para poder tener un registro de todos los archivos eliminados por el módulo. Tendrá que recuperar los archivos eliminados de las copias de seguridad.
- **Continuar la exploración.** Elija esta respuesta para que el módulo continúe la exploración sin emprender acción alguna contra los virus que detecta. Si también activa la función de generación de informes de Exploración de transferencias, el programa registrará los nombres de los virus que detecte y de los archivos infectados para que pueda eliminarlos tan pronto como tenga la oportunidad.

Utilice esta opción sólo si tiene pensado dejar el equipo sin supervisión mientras el módulo comprueba si hay virus.

3. Haga clic en la pestaña Alerta para seleccionar otras opciones del módulo Explorador de elementos descargados. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración de descarga, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA**: Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Alerta

Una vez configuradas las opciones de respuesta deseadas en la página Acción, el módulo Exploración de transferencias puede buscar y eliminar automáticamente los virus del sistema, conforme los vaya encontrando, sin casi ninguna intervención posterior. Sin embargo, si desea que el módulo le avise cuando encuentre un virus para que pueda emprender la acción apropiada, configúrelo de modo que envíe un mensaje de alerta.

Siga estos pasos:

1. Haga clic en la ficha Alerta del módulo Exploración de transferencias para mostrar la página de propiedades adecuada.

2. Active la casilla de verificación **Notificar al Administrador de alertas** para que el módulo envíe mensajes de alerta al Administrador de alertas para su distribución.

   El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que el módulo Exploración de transferencias envíe satisfactoriamente estos mensajes de alerta, deberá configurar también la utilidad de configuración del cliente del Administrador de alertas.

   Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

- **NOTA:** Al desactivar esta casilla de verificación, se indica al módulo Exploración de transferencias que no envíe un mensaje de alerta a través del Administrador de alertas, sin que ello afecte a otros mensajes de alerta configurados en esta página de propiedades.

3. Active la casilla de verificación **Alerta sonora** para que el módulo emita un tono cuando encuentre un archivo infectado.

   Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**. El módulo hará sonar un sonido estándar de alerta del sistema o el archivo .WAV que tenga configurado el equipo.

4. Active la casilla de verificación **Mostrar mensaje personalizado** para que el módulo añada un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

   Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

5. Escriba el mensaje que debe mostrar el módulo en el cuadro de texto provisto para ello. Puede escribir 250 caracteres como máximo.

6. Haga clic en la ficha Informe para seleccionar otras opciones del módulo Exploración de transferencias. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de exploración de descarga, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Informe

El módulo Exploración de transferencias enumera las opciones de configuración actuales y resume todas las acciones que emprende durante las operaciones de exploración en un archivo de registro denominado WEBINET.TXT. Puede configurar el módulo para que escriba su registro en ese archivo o puede utilizar cualquier editor de texto para crear un archivo de texto con este fin. Después, podrá abrir e imprimir el archivo de registro para examinarlo desde cualquier editor de texto. Utilice la página de propiedades Informe para determinar qué información debe incluir el módulo en su archivo de registro.

El archivo WEBINET.TXT puede ser una importante herramienta de administración para realizar un seguimiento de la actividad de los virus en el sistema y tomar nota de la configuración utilizada para detectar y responder a las infecciones que encuentre el módulo Exploración de transferencias. También puede utilizar los informes de incidentes que se registran en el archivo para determinar qué archivos tiene que reemplazar a partir de las copias de seguridad, cuáles debe examinar de los que se encuentran en el área de cuarentena y cuáles debe eliminar del equipo.

Para configurar el módulo Exploración de transferencias de modo que anote sus acciones en un archivo de registro, siga estos pasos:

1. Haga clic en la ficha Informe del módulo Exploración de transferencias para mostrar la página de propiedades adecuada.
2. Active la casilla de verificación **Registrar en archivo**.

   De manera predeterminada, el módulo Exploración de transferencias escribe la información de registro en el archivo WEBINET.TXT ubicado en el directorio de programa de VirusScan.

   Puede escribir un nombre y una ruta de acceso distintos en el cuadro de texto correspondiente o hacer clic en **Examinar** para encontrar un archivo adecuado en el disco duro o en la red. Puede utilizar un archivo diferente, pero debe existir el archivo de texto. El módulo no creará un archivo nuevo.
3. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente. Si no activa esta casilla de verificación, el tamaño del archivo de registro puede aumentar hasta donde el espacio en disco o el sistema de archivos lo permita.

Escriba un valor entre 10 KB y 999 KB. De manera predeterminada, el módulo Exploración de transferencias limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, el módulo eliminará el registro existente y comenzará de nuevo desde el punto en el que se detuvo.

4. Active las casillas de verificación que correspondan a la información que desea que el módulo incluya en el archivo de registro. Normalmente, el módulo registrará los datos al término de la operación de exploración o al apagar el sistema.

   Puede elegir la información que desea registrar:

   - **Detección de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo encuentre durante cada operación de exploración. Desactive la casilla de verificación para no incluir esta información.
   - **Eliminación de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo elimine en cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información.
   - **Desplazamiento de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que el módulo mueve a una carpeta de cuarentena en cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información.
   - **Configuración de sesión**. Active esta casilla de verificación para que el archivo de registro incluya las opciones de configuración utilizadas para el módulo en cada sesión de exploración. Desactive esta casilla de verificación para no incluir esta información.
   - **Resumen de sesión**. Active esta casilla de verificación para que el archivo de registro haga un resumen de las acciones emprendidas por el módulo en cada operación de exploración.

     Si elige esta opción, el registro incluirá:

     – El número de archivos examinados por el módulo.

     – El número de archivos infectados limpiados por el módulo.

     – El número de archivos infectados eliminados por el módulo.

     – El número de archivos infectados trasladados por el módulo a una carpeta de cuarentena.

     – La configuración del módulo Exploración de transferencias.

     Desactive la casilla de verificación para no incluir esta información.

5. Haga clic en otra ficha para modificar cualquiera de las opciones de configuración del módulo Exploración de transferencias o en uno de los iconos situados en el lateral del cuadro de diálogo Propiedades de exploración de descarga para seleccionar las opciones de otro módulo.

   Para guardar los cambios del módulo Exploración de transferencias sin cerrar el cuadro de diálogo, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Configuración del módulo Filtro de Internet

Aunque los objetos de Java y ActiveX incluyen garantías diseñadas para evitar daños al sistema informático, algunos programadores han desarrollado objetos que utilizan funciones antiguas de Java o ActiveX para causar daños de todo tipo al sistema.

Objetos peligrosos como éstos a menudo pueden ocultarse en los sitios Web hasta que un usuario los visita y los descarga a su sistema, normalmente sin darse cuenta de que existen. La mayoría del software de visualizador incluye una función que permite bloquear totalmente los subprogramas de Java o los controles de ActiveX, o activar las funciones de seguridad que autentican los objetos antes de descargarlos al sistema. Sin embargo, estos enfoques pueden privarle de las ventajas interactivas que ofrecen los sitios Web que visita bloqueando sin discriminación todos los objetos, ya sean peligrosos o no.

El módulo Filtro de Internet permite un enfoque más acertado. Recurre a una base de datos actualizada de los objetos de los que se sabe que causan daños con el fin de examinar las clases de Java y los controles de ActiveX que se encuentran al navegar por Internet.

Al encontrar un virus, el módulo puede preguntarle qué debe hacer o bloquear automáticamente el objeto o sitio. Puede configurarlo para que informe de lo que ha hecho mediante un mensaje de alerta cuando emprende la acción o en un archivo de registro que puede revisar cuando lo crea conveniente.

Para seleccionar las opciones, haga clic en el icono de Filtro de Internet situado en el lado izquierdo del cuadro de diálogo Propiedades de VShield para ver las páginas de propiedades correspondientes a este módulo.

- **NOTA:** El icono de Filtro de Internet no aparecerá a menos que se haya utilizado la opción de instalación personalizada para instalar el software de VirusScan y se haya decidido instalar el componente Exploración de Internet.

Selección de las opciones de Detección

En principio, el módulo Filtro de Internet da por supuesto que el usuario desea bloquear todos los objetos y sitios peligrosos incluidos en la base de datos con el fin de evitar que los encuentre de manera fortuita. Esta opción proporciona la mejor protección contra objetos peligrosos, pero permite al usuario hacer uso de los demás objetos ubicados en los sitios de Internet que visite.

Para cambiar las opciones de configuración, siga estos pasos:

1. Compruebe que esté activada la casilla de verificación Activar filtro Java y ActiveX.

   Esto activará las demás opciones de la página de propiedades.

2. Especifique los objetos que debe examinar el módulo Filtro de Internet. Las opciones disponibles son:

   - **Controles de ActiveX**. Active esta casilla de verificación para que el módulo busque y bloquee los controles ActiveX u .OCX peligrosos.
   - **Clases de Java**. Active esta casilla de verificación para que el módulo busque y bloquee las clases de Java o los subprogramas escritos en Java de índole peligrosa.

   El módulo Filtro de Internet comparará los objetos encontrados al visitar los sitios de Internet con una base de datos interna que contiene las características de los objetos de los que se sabe que causan daños. Al encontrar una coincidencia, el módulo puede advertir al usuario y dejar que él decida qué hacer o puede impedir automáticamente la descarga del objeto.

3. Indique al módulo los sitios que debe filtrar. El programa utiliza una lista de sitios de Internet peligrosos para decidir qué sitios debe evitar el visualizador. Para activar esta función y añadir a la lista de sitios "prohibidos", puede proceder de dos maneras:

- **Direcciones de IP a bloquear.** Active esta casilla de verificación para indicar al módulo que identifique los sitios de Internet peligrosos en base a sus direcciones IP (Protocolo de Internet). Para ver o designar las direcciones que el módulo deberá prohibir, haga clic en **Configurar** para abrir el cuadro de diálogo Direcciones IP prohibidas.

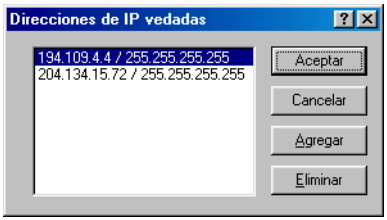

Figura 4-18. Cuadro de diálogo Direcciones IP prohibidas

El cuadro de diálogo Direcciones IP prohibidas identifica las direcciones IP (Protocolo de Internet) que debe bloquear el módulo Filtro de Internet cuando algún usuario intente conectarse a ellas.

De manera predeterminada, la lista incluye dos sitios que descargan objetos Java o ActiveX dañinos al equipo en cuanto se conecte. Podrá añadir otros sitios y, a continuación, proteger con una contraseña la configuración para asegurarse de que otros usuarios no los eliminen.

Cada dirección se compone de cuatro grupos numéricos de uno a tres dígitos cada uno, con el siguiente formato:

123.123.123.123

El módulo Filtro de Internet puede utilizar este número para identificar un equipo específico o una red de equipos en Internet e impedir que el visualizador se conecte a ellos. Cada grupo de números puede ir de 0 a 255. La primera serie de números es la dirección del dominio del sitio prohibido, el número que se utiliza para encontrarlo en Internet, y la segunda es una "máscara de subred".

Una máscara de subred es una manera de "reasignar" un grupo de direcciones de equipo dentro de una red interna. El módulo muestra una máscara de subred predeterminada: 255.255.255.255. En la mayoría de los casos, no deberá cambiar este número pero si sabe que un nodo de red determinado en el sitio que visita es fuente de peligro, posiblemente tenga que introducir una máscara de subred para conservar el acceso a otros equipos en este sitio.

Para cambiar esta lista:

– Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar dirección de IP.

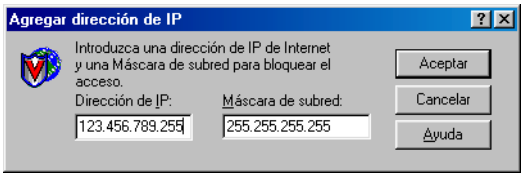

Figura 4-19. Cuadro de diálogo Agregar dirección de IP

A continuación, siga estos pasos:

a. Escriba en el cuadro de diálogo situado a la izquierda la dirección IP (Protocolo de Internet) que desee agregar a la lista de direcciones IP prohibidas. Asegúrese de separar los grupos de números de la dirección mediante puntos.

b. Escriba en el cuadro de texto a la derecha la máscara de subred asociada con la dirección IP que desee agregar a la lista de direcciones IP prohibidas, siempre y cuando conozca el valor correcto de la máscara de subred correspondiente al lugar que desee evitar. De lo contrario, deje el valor predeterminado.

c. Haga clic en **Aceptar** para volver al cuadro de diálogo Direcciones de IP prohibidas.

– Seleccione uno de los elementos que aparecen y, a continuación, haga clic en **Eliminar** para eliminarlo de la lista.

Una vez modificada la lista de direcciones prohibidas de modo que incluya todas las direcciones que desee bloquear, haga clic en **Aceptar** para volver al cuadro de diálogo Propiedades de filtro de Internet.

- **URL de Internet a bloquear.** Active esta casilla de verificación para indicar al módulo que identifique los sitios de Internet peligrosos en base a su dirección URL (Uniform Resource Locator). Para ver o seleccionar las direcciones que el módulo deberá prohibir, haga clic en **Configurar** para abrir el cuadro de diálogo de direcciones URL prohibidas.

Figura 4-20. Cuadro de diálogo URL prohibidos

El cuadro de diálogo de direcciones URL prohibidas identifica las direcciones URL (Uniform Resource Locator) que debe bloquear el módulo Filtro de Internet cuando algún usuario intente conectarse a ellas.

De manera predeterminada, la lista incluye dos nombres de dominio que descargan objetos Java o ActiveX dañinos al equipo en cuanto se conecte. Podrá añadir otros nombres de dominio y, a continuación, proteger con una contraseña la configuración para asegurarse de que otros usuarios no los eliminen.

Las direcciones URL especifican el nombre de dominio y la ubicación de un equipo en Internet, normalmente junto con el "protocolo de transporte" que desea utilizar para solicitar un recurso de ese equipo. Una dirección URL completa de un sitio Web tendría, por ejemplo, este aspecto:

http://www.domain.com

La dirección URL completa indica al visualizador que solicite el recurso a través del Protocolo de transporte de hipertexto ("http://") de un equipo denominado "www" en un dominio de red denominado "domain.com". Otros protocolos de transporte incluyen "ftp://" y "gopher://". El Sistema de nombres de dominio de Internet traduce las direcciones URL en direcciones IP utilizando una base de datos actualizada y centralizada de referencias cruzadas.

Para añadir un sitio a esta lista, deberá escribir el nombre de dominio, ya que el módulo dará por supuesto que hace referencia al protocolo HTTP. Para cambiar esta lista:

– Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar URL. A continuación, escriba la dirección URL que desee agregar a la lista de direcciones URL prohibidas en el cuadro de diálogo que aparece. Haga clic en **Aceptar** para volver al cuadro de diálogo Direcciones de IP prohibidas.

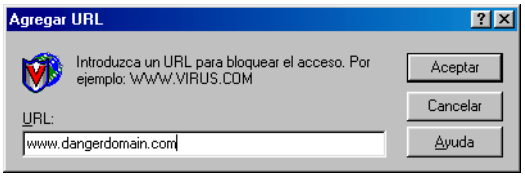

Figura 4-21. Cuadro de diálogo Agregar URL

– Seleccione uno de los elementos que aparecen y, a continuación, haga clic en **Eliminar** para eliminarlo de la lista.

Una vez modificada la lista de direcciones prohibidas de modo que incluya todas las direcciones que desee bloquear, haga clic en **Aceptar** para volver al cuadro de diálogo Propiedades de filtro de Internet.

4. Haga clic en la ficha Acción para seleccionar otras opciones del módulo Filtro de Internet. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de filtro de Internet, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Acción

Cuando el módulo Filtro de Internet encuentra un objeto peligroso o un sitio prohibido, puede responder preguntándole si debe bloquear el objeto o sitio o bloqueándolo automáticamente. Utilice la página de propiedades de Acción para especificar la acción que debe emprender el módulo.

De manera predeterminada, el módulo le deja tomar la decisión.

Elija una respuesta en la lista **Cuando se encuentra un objeto potencialmente peligroso**. Podrá elegir entre las siguientes opciones:

- **Consultar al usuario antes de realizar acción.** Elija esta respuesta para que el módulo pregunte si debe bloquear o permitir el acceso a un objeto o sitio peligroso.

- **NOTA:** Si selecciona **Consultar al usuario antes de realizar acción** en la lista, haga clic en la ficha Alerta para especificar si el módulo Filtro de Internet debe advertirle mediante un mensaje, una señal sonora o ambos.

- **Negar el acceso a objetos.** Elija esta respuesta para que el módulo bloquee automáticamente los objetos o sitios peligrosos. El programa lo hará en base al contenido de su propia base de datos y toda la información sobre los sitios que haya agregado.

Haga clic en la ficha Alerta para seleccionar otras opciones del módulo Filtro de Internet. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de filtro de Internet, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Alerta

Una vez configuradas las opciones de respuesta deseadas en la página Acción, el módulo Filtro de Internet puede buscar y bloquear automáticamente los objetos dañinos o los sitios de Internet peligrosos, conforme los vaya encontrando, sin casi ninguna intervención posterior. Sin embargo, si desea que el módulo le advierta cuando encuentra un objeto dañino para que pueda emprender la acción apropiada, configúrelo de modo que envíe un mensaje de alerta.

Siga estos pasos:

1. Haga clic en la ficha Alerta del módulo Filtro de Internet para mostrar la página de propiedades adecuada.
2. Active la casilla de verificación **Notificar al Administrador de alertas** para que el módulo envíe mensajes de alerta al Administrador de alertas para su distribución.

   El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que el módulo Filtro de Internet envíe satisfactoriamente estos mensajes de alerta, deberá configurar también la utilidad de configuración del cliente del Administrador de alertas.

   Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

- **NOTA:** Al desactivar esta casilla de verificación, se indica al módulo Filtro de Internet que no envíe un mensaje de alerta a través del Administrador de alertas, sin que ello afecte a otros mensajes de alerta configurados en esta página de propiedades.

3. Active la casilla de verificación **Alerta sonora** para que el módulo emita un tono cuando encuentre un archivo infectado.

   Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**. El módulo hará sonar un sonido estándar de alerta del sistema o el archivo .WAV que tenga configurado el equipo.

4. Active la casilla de verificación **Mostrar mensaje personalizado** para que el módulo añada un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

   Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

5. Escriba el mensaje que debe mostrar el módulo en el cuadro de texto provisto para ello. Puede escribir 250 caracteres como máximo.

6. Haga clic en la ficha Informe para seleccionar otras opciones del módulo Filtro de Internet. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de filtro de Internet, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Informe

El módulo Filtro de Internet registra el número de objetos Java y ActiveX explorados y bloqueados en un archivo de registro denominado WEBFLTR.TXT. El mismo archivo registra el número de sitios de Internet visitados mientras estaba activo el módulo y el número de sitios peligrosos que el programa impidió visitar al visualizador.

Puede configurar el módulo para que escriba su registro en el archivo predeterminado o puede utilizar cualquier editor de texto para crear un archivo de texto con este fin. Después, podrá abrir e imprimir el archivo de registro para examinarlo desde cualquier editor de texto. Utilice la página de propiedades Informe para designar el archivo que desee utilizar como el registro de Filtro de Internet y determinar el tamaño tolerable de ese archivo.

El archivo WEBFLTR.TXT puede ser una importante herramienta de administración para realizar un seguimiento de la actividad del software perjudicial en el sistema y tomar nota de la configuración utilizada para detectar y bloquear los objetos o sitios dañinos encontrados por el módulo.

Para configurar el módulo Filtro de Internet de modo que anote sus acciones en un archivo de registro, siga estos pasos:

1. Haga clic en la ficha Informe del módulo Filtro de Internet para mostrar la página de propiedades adecuada.
2. Active la casilla de verificación **Registrar en archivo**.

   De manera predeterminada, el módulo escribe la información de registro en el archivo WEBFLTR.TXT ubicado en el directorio de programa de VirusScan. Puede escribir un nombre y una ruta de acceso distintos en el cuadro de texto correspondiente o hacer clic en **Examinar** para encontrar un archivo adecuado en el disco duro o en la red.
3. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente.

   Escriba un valor entre 10 KB y 999 KB. De manera predeterminada, el módulo limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, el módulo eliminará el registro existente y comenzará de nuevo desde el punto en el que se detuvo.
4. Haga clic en otra ficha para modificar cualquiera de los valores del módulo Filtro de Internet o en uno de los iconos situados en el lateral del cuadro de diálogo Propiedades de filtro de Internet para seleccionar las opciones de otro módulo.

   Para guardar los cambios del módulo Filtro de Internet sin cerrar el cuadro de diálogo, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Configuración del módulo Seguridad

Para evitar que la configuración seleccionada para cada módulo de VShield sufra modificaciones no autorizadas, podrá proteger una o todas las páginas de propiedades con una contraseña. Los administradores de sistema pueden impedir que los usuarios de la red desactiven el explorador VShield (consulte el Paso 4 en la página 110 para obtener más información) y proteger la configuración con una contraseña con el fin de imponer fácil y eficazmente una rigurosa política de seguridad antivirus.

Utilice el módulo Seguridad para asignar una contraseña y seleccionar las páginas que desee proteger.

Activación de la protección con contraseña

El módulo Seguridad de VShield no está activado de manera predeterminada ya que necesita saber la contraseña que el usuario desea asignar a la configuración.

Para activar y configurar la protección con contraseña del módulo Seguridad, siga estos pasos:

1. Active la casilla de verificación **Activar protección con contraseña**.

   Se activarán las demás opciones de la página de propiedades.

2. Deberá decidir si desea proteger las páginas de propiedades de todos los módulos de VShield o sólo páginas individuales. Podrá elegir entre las siguientes opciones:

   - **Todas las opciones de todas las páginas de propiedades.** Seleccione este botón para bloquearlo todo inmediatamente.
   - **Sólo páginas de propiedades seleccionadas.** Elija este botón para seleccionar las páginas de propiedades de módulos individuales que desee bloquear. Las demás fichas del cuadro de diálogo Propiedades de seguridad permiten designar páginas individuales.

3. Escriba la contraseña que desee utilizar para bloquear las configuraciones. Escriba una combinación de hasta 20 caracteres en el cuadro de texto superior del área Contraseña y, a continuación, escriba exactamente la misma combinación en el cuadro de texto inferior para confirmar la contraseña elegida.

E **IMPORTANTE:** La protección con contraseña del explorador VShield es distinta de la que se puede asignar a las tareas en la Consola de VirusScan o a las configuraciones en la aplicación VirusScan. Elegir una contraseña para un componente no significa que esa misma contraseña se asigne a otros componentes. Se deberán seleccionar de manera independiente contraseñas para cada uno de los componentes.

4. Haga clic en cualquiera de las demás fichas del módulo Seguridad para proteger las páginas de propiedades individuales. Para guardar la contraseña sin cerrar el cuadro de diálogo Propiedades de seguridad, haga clic en **Aplicar**. Si opta por proteger todas las páginas de propiedades en todos los módulos y desea cerrar el cuadro de diálogo, haga clic en **Aceptar**. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   • **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Introducción de la contraseña para las opciones de configuración

Tras proteger la configuración con una contraseña, el módulo Seguridad le pedirá que escriba esa contraseña cada vez que abra el cuadro de diálogo Propiedades de VShield.

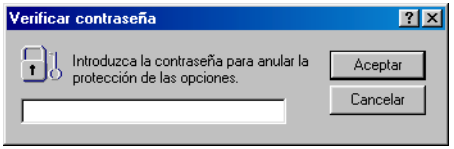

Figura 4-22. Cuadro de diálogo Verificar contraseña

Escriba la contraseña seleccionada en el cuadro de texto correspondiente y, a continuación, haga clic en **Aceptar** para obtener acceso al cuadro de diálogo Propiedades de VShield.

Protección de páginas de propiedades individuales

Si elige **Sólo páginas de propiedades seleccionadas** en la página Contraseña del módulo Seguridad, podrá seleccionar las opciones de configuración que desee bloquear para módulos individuales.

Siga estos pasos:

1. Haga clic en la ficha correspondiente al *módulo* cuya configuración desee proteger. Si no ve la ficha deseada, haga clic en  o en  para que aparezca. Aparecerá una página representativa.

2. Seleccione la configuración que desee proteger en la lista que aparece.

   Podrá proteger una o todas las páginas de propiedades de un módulo. Las páginas de propiedades protegidas se indican mediante un icono de candado cerrado  en la lista de seguridad que se muestra. Para eliminar la protección de una página de propiedades, haga clic en el icono de candado cerrado para abrirlo  .

3. Seleccione tantas páginas de propiedades como desee proteger en cada módulo.

4. Para guardar la contraseña sin cerrar el cuadro de diálogo Propiedades de seguridad, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Utilización del menú de acceso directo de VShield

El explorador VShield agrupa varios de sus comandos más comunes en un menú de acceso directo asociado a su icono en la bandeja del sistema. Haga doble clic en este icono para mostrar el cuadro de diálogo Estado de VShield. Haga clic con el botón derecho del ratón para mostrar estos comandos:

- **Estado.** Seleccione esta opción para abrir el cuadro de diálogo Estado de VShield.
- **Propiedades.** Elija esta opción y, a continuación, seleccione uno de los módulos que aparecen en la lista para abrir el cuadro de diálogo Propiedades de VShield en la página de propiedades de ese módulo.
- **Activación rápida.** Elija esta opción y, a continuación, seleccione uno de los módulos de VShield que aparecen en la lista para activarlo o desactivarlo. Los módulos que aparecen en el menú con marcas de verificación se encuentran activados, mientras que aquellos que aparecen sin ellas se encuentran desactivados. Si utiliza este método para desactivar un módulo, dicho módulo permanecerá desactivado hasta que reinicie el equipo.

- **Acerca de.** Seleccione esta opción para mostrar el número de serie y el número de versión del explorador VShield, el número de versión y la fecha de creación de los actuales archivos .DAT que están en uso y un aviso acerca del copyright de McAfee VirusScan.
- **Salir.** Elija esta opción para detener todos los módulos de VShield y para descargar todo el explorador VShield de la memoria.

Desactivación o detención del explorador VShield

Al final de la instalación de VirusScan, el programa de instalación pregunta si desea activar el explorador VShield en ese momento. Si la respuesta es afirmativa, el explorador VShield deberá cargarse inmediatamente en la memoria y comenzar a funcionar con un conjunto de opciones predeterminadas que proporcionan una protección antivirus básica. Si la respuesta es negativa, el explorador VShield se cargará automáticamente la próxima vez que reinicie el equipo.

Cuando se inicia por primera vez el explorador VShield, aparece un icono en la bandeja del sistema de Windows que indica los módulos que están activos.

Podrá detener completamente el explorador, lo cual significa que desactivará todos los módulos de VShield y eliminará el explorador de la memoria. El icono de VShield desaparecerá de la bandeja del sistema. En ese momento, podrá reiniciar el explorador sólo desde el panel de control de VirusScan, desde la Consola de VirusScan o reiniciando el equipo si ha configurado VShield para que se cargue al iniciar el equipo.

No es lo mismo que desactivar el explorador, lo cual implica desactivar uno o varios de sus módulos e impedir que esos módulos se ejecuten durante una operación de exploración. El explorador no se detiene y no se descarga de la memoria del equipo. El explorador VShield puede permanecer activo en la memoria incluso cuando ninguno de sus módulos está activado. En este estado, el explorador conservará un icono  en la bandeja del sistema de Windows que podrá utilizar para volver a activarlo.

Configuración del explorador para que no se inicie automáticamente

Si no desea que el explorador VShield se inicie automáticamente, podrá configurarlo de ese modo desde el panel de control de VirusScan.

Siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.

2. Localice y haga doble clic en el panel de control de VirusScan para abrirlo.
3. Haga clic en la ficha Componentes.
4. Desactive la casilla de verificación **Cargar VShield al inicio** que parece en la parte superior de la página de propiedades Componentes.
5. Haga clic en **Aceptar** para cerrar el panel de control.

El explorador VShield no se detendrá ni se descargará en ese momento, pero no se iniciará la próxima vez que encienda el equipo.

Detención completa del explorador VShield

Existe la posibilidad de detener completamente el explorador VShield, es decir, desactivarlo y eliminarlo de la memoria, de tres modos diferentes. Una vez detenido el explorador, podrá reactivarlo con sólo reiniciarlo o reiniciar el equipo.

Método 1: Desde el menú de acceso directo de VShield

Siga estos pasos:

1. Haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo.
2. Seleccione **Salir**.

   El explorador VShield se detendrá y se descargará automáticamente de la memoria. El icono de VShield desaparecerá de la barra de tareas de Windows.

Método 2: Desde la Consola de VirusScan

Siga estos pasos:

1. Haga doble clic en el icono de la Consola de VirusScan en la bandeja del sistema Windows para llevar la ventana de la Consola al primer plano.

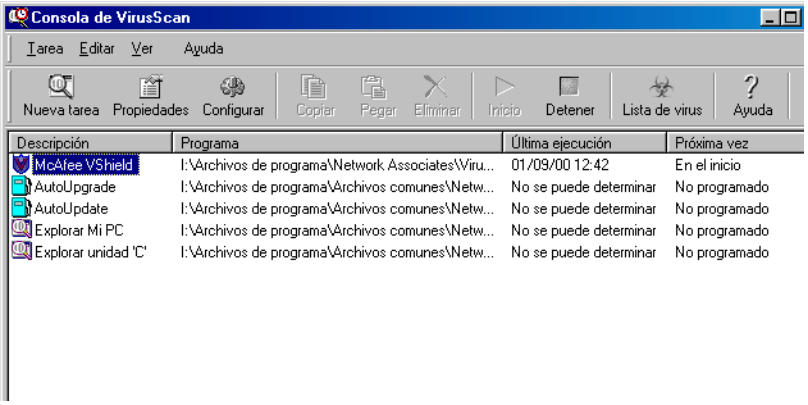

Figura 4-23. Ventana de la Consola de VirusScan

2. Seleccione VShield en la lista de tareas y, a continuación, elija **Desactivar** en el menú **Tarea**.

   La Consola detendrá el explorador VShield y todos sus módulos además de descargarlos de la memoria. El icono de VShield desaparecerá de la barra de tareas de Windows.

3. Haga clic en el botón de minimizar o de cerrar en la esquina superior derecha de la ventana de la Consola para reducirla a un icono en la bandeja del sistema.

- **NOTA:** No elija **Salir** en el menú **Tarea**. De esta manera se cerrará la Consola y se descargará de la memoria. Para ejecutar las tareas programadas, la Consola deberá estar activa.

Método 3: Desde el panel de control de VirusScan

Siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.
2. Localice y haga doble clic en el panel de control de VirusScan para abrirlo.

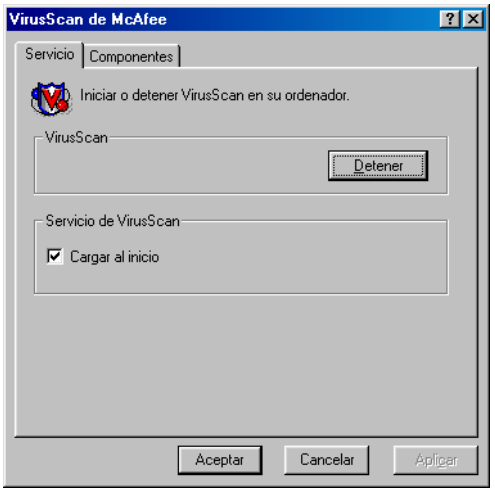

Figura 4-24. Panel de control de VirusScan: página Servicio

3. Haga clic en **Detener** en la página Servicio.

   Todos los componentes activos de VirusScan se detendrán, se cerrarán todos los cuadros de diálogo o ventanas abiertos, se eliminarán todos sus iconos de la bandeja del sistema de Windows y se descargarán de la memoria.
4. Haga clic en **Aceptar** para cerrar el panel de control.

Desactivación del explorador VShield y sus módulos

Podrá utilizar cualquiera de los tres métodos para desactivar cualquiera de los módulos de VShield, es decir, desactivar el módulo pero sin eliminarlo de la memoria del explorador. Una vez desactivado un módulo, podrá reactivarlo de una manera muy similar a la utilizada para desactivarlo.

Método 1: Desde el menú de acceso directo de VShield

Siga estos pasos:

1. Haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo.
2. Seleccione **Activación rápida**.
3. Elija uno de los nombres de módulo que aparecen con una marca de verificación al lado para desactivarlo. Los nombres de módulo que tienen una marca de verificación están activos. Y los que no tienen marca de verificación están inactivos. Este método permite desactivar un módulo sólo por el tiempo que dura una operación de exploración o hasta que vuelva a activarlo. El módulo volverá a iniciarse cuando reinicie el equipo.

   Dependiendo de la combinación de módulos que active, el icono de VShield mostrará un estado diferente.

Método 2: Desde el cuadro de diálogo Estado de exploración del sistema

Siga estos pasos:

1. Haga doble clic en el icono de VShield en la bandeja del sistema de Windows para abrir el cuadro de diálogo Estado de exploración de sistema.

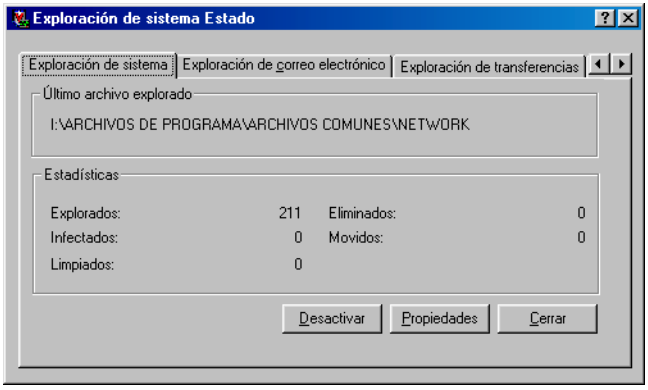

Figura 4-25. Cuadro de diálogo Estado de exploración del sistema de VShield

2. Para cada módulo que desee desactivar, haga clic en la ficha correspondiente y, a continuación, en **Desactivar**. El mismo botón en la página de propiedades de los módulos inactivos aparecerá con el texto **Activar**.
3. Haga clic en **Cerrar** para cerrar el cuadro de diálogo.

Dependiendo de la combinación de módulos que active, el icono de VShield mostrará un estado diferente.

Método 3: Desde el cuadro de diálogo Propiedades de VShield

Siga estos pasos:

1. Haga clic con el botón derecho del ratón en el icono de VShield en la bandeja del sistema de Windows para mostrar el menú de acceso directo.
2. Seleccione **Propiedades** y, a continuación, elija el nombre de un módulo para abrir el cuadro de diálogo Propiedades de VShield.
3. Para cada módulo que desee desactivar, haga clic en el icono correspondiente que aparece a la izquierda del cuadro de diálogo y, a continuación, haga clic en la ficha Detección.
4. Desactive la casilla de verificación **Activar** que aparece en la parte superior de cada página.

   Procediendo de este modo, el explorador desactivará ese módulo y no estará disponible ninguna de las opciones de configuración de esa página. Dependiendo de los módulos que desactive, el icono de VShield mostrará un estado diferente.

   Si desactiva todos los módulos, el explorador mostrará  en la bandeja del sistema de Windows, a menos que desactive la casilla de verificación **Mostrar icono en la Barra de tareas** en la página de propiedades Detección de exploración del sistema. En ese caso, VShield no mostrará ningún icono en la bandeja del sistema.

   Al utilizar este método para desactivar el módulo, el estado desactivado será el estado "predeterminado" del módulo. Si más adelante utiliza el menú de acceso directo para activar el módulo, éste permanecerá activado sólo hasta que reinicie el software de VirusScan en el equipo.

Seguimiento de la información de estado del software de VShield

Una vez activado y configurado el explorador VShield, éste funcionará de manera continua en segundo plano, a la espera de explorar los correos electrónicos que reciba, los archivos que ejecute o descargue, o los objetos Java y ActiveX que encuentre.

Para ver un resumen en tiempo real de su progreso:

1. Haga doble clic en el icono de VShield en la bandeja del sistema para abrir el cuadro de diálogo Estado.

2. Haga clic en la ficha correspondiente al módulo de programa cuyo progreso desee comprobar.

   La información que facilitará cada módulo es la siguiente:

   - **Exploración de sistema**. Este módulo facilita el número de archivos explorados, el número de archivos infectados encontrados y el número de archivos limpiados, movidos o eliminados.
   - **Exploración de correo electrónico**. Este módulo facilita el número de archivos explorados, el número de infecciones encontradas y el número de archivos movidos o eliminados.
   - **Exploración de transferencias**. Este módulo facilita el número de archivos explorados, el número de infecciones encontradas y el número de archivos movidos o eliminados.
   - **Filtro de Internet**. Este módulo facilita el número de objetos Java y ActiveX o sitios de Internet explorados, prohibidos o "esquivados".

   Para ver una breve descripción de cada uno de los elementos que aparecen en esta página, haga clic con el botón derecho del ratón en una figura o etiqueta y, a continuación, seleccione **¿Qué es esto?** en el menú de acceso directo que aparece o haga clic en el botón **?** que aparece en la esquina superior derecha del cuadro de diálogo y, por último, haga clic en el elemento cuya descripción desee ver.

   Si está activada la función de generación de informes, el explorador VShield incluirá la misma información en el archivo de registro de cada módulo.

Otras funciones disponibles en este cuadro de diálogo son:

- **Activar o desactivar los módulos**. Haga clic en la ficha correspondiente al componente de programa que desee activar o desactivar y, a continuación, haga clic en **Activar** para iniciarlo. Haga clic en **Desactivar** para desactivarlo.
- **Abrir el cuadro de diálogo Propiedades de VShield**. Haga clic en la ficha correspondiente al componente de programa que desee configurar y, a continuación, haga clic en **Propiedades** para abrir el cuadro de diálogo Propiedades de VShield de ese módulo.

Visualización de la información sobre el estado de las tareas de VShield

Existe también la posibilidad de ver información estadística en el cuadro de diálogo Propiedades de tarea de cada módulo de VShield.

Para ver esta información, siga estos pasos:

1. Haga doble clic en el icono de la Consola de VirusScan en la bandeja del sistema Windows para llevar la ventana de la Consola al primer plano.
2. Haga doble clic en la tarea VShield en la lista de tareas para abrir el cuadro de diálogo Propiedades de tarea.

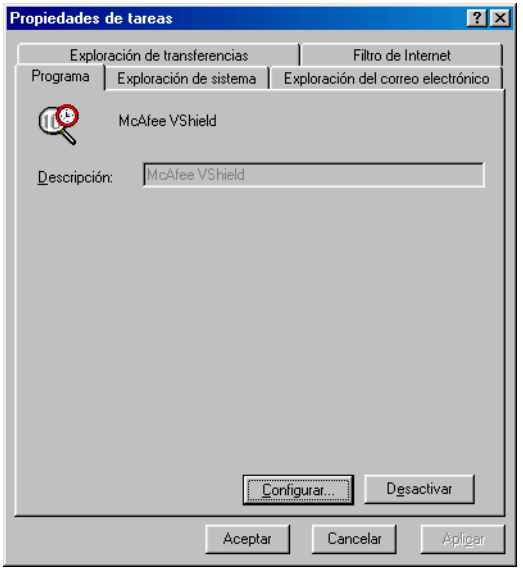

Figura 4-26. Cuadro de diálogo Propiedades de tarea de VShield

3. Haga clic en la ficha correspondiente al componente de programa que desee activar o desactivar o cuyo progreso desee comprobar.

   La página de estado mostrará una lista con los resultados de la última exploración que llevó a cabo esta tarea, así como el nombre del último archivo explorado. Para ver una breve descripción de cada uno de los elementos que aparecen en esta página, haga clic con el botón derecho del ratón en una figura o etiqueta y, a continuación, seleccione **¿Qué es esto?** en el menú de acceso directo que aparece o haga clic en el botón **?** que aparece en la esquina superior derecha del cuadro de diálogo y, por último, haga clic en el elemento cuya descripción desee ver. Estas pantallas *no* se actualizarán en tiempo real.

   Si está activada la función de generación de informes, el explorador VShield incluirá la misma información en el archivo de registro de cada módulo.

Uso de la aplicación VirusScan 5

¿Qué es la aplicación VirusScan?

Los productos antivirus para equipos individuales de McAfee VirusScan utilizan dos métodos generales para proteger el sistema. El primer método, exploración en segundo plano, funciona constantemente, buscando virus mientras el usuario utiliza el equipo para su trabajo diario. En el producto VirusScan, el explorador VShield realiza esta función.

El segundo método depende del usuario. El usuario decide cuándo y dónde el software debe buscar virus y, a continuación, determina y ejecuta las operaciones de exploración que mejor se ajusten a sus necesidades. Puede ejecutar operaciones de exploración sucesivas o simultáneas, crear diferentes configuraciones y especificar diferentes objetivos de exploración para cada operación y guardar dichas configuraciones en archivos que se puedan exportar para su utilización en un futuro.

En otras fuentes este segundo método se denomina "exploración a petición". El término "a petición" significa que, como usuario, usted decide cuándo debe iniciar y finalizar una operación de exploración, qué objetivos debe examinar, qué debe hacer cuando se detecta un virus o cualquier otro aspecto relacionado con del funcionamiento de la exploración. Por el contrario, otros componentes de VirusScan funcionan automáticamente o de acuerdo con un programa establecido por el usuario.

El nombre VirusScan se aplica a todos los componentes de programas antivirus de escritorio que se describen en esta *Guía del usuario*. La aplicación VirusScan funciona en dos modos:

- **La interfaz de VirusScan "Clásico"**. Este modo permite un inicio y ejecución rápidos, con un mínimo de opciones de configuración, pero con toda la eficacia que proporciona el motor de exploración antivirus de VirusScan.
- **La interfaz de VirusScan Avanzado**. Este modo agrega flexibilidad a las opciones de configuración del programa, incluida la capacidad para ejecutar más de una operación de exploración de forma simultánea.

Este capítulo describe cómo utilizar el software de VirusScan tanto en el modo Clásico como en el Avanzado.

¿Por qué utilizar la aplicación VirusScan?

Mantener un entorno informático seguro significa explorarlo periódicamente en busca de virus. Según la frecuencia con que intercambie disquetes con otros usuarios, comparta archivos a través de la red de área local o se comunique con otros equipos a través de Internet, la "periodicidad" de la exploración puede significar tan poco como una vez al mes o tan a menudo como varias veces al día. Entre los hábitos correctos se incluyen, además, la exploración antes de hacer una copia de seguridad de los datos, antes de instalar un software nuevo o una versión nueva, especialmente si se ha descargado el software de otro equipo, y al encender o apagar el equipo después de una sesión.

Utilice el explorador VShield para explorar la memoria del equipo y mantener un nivel constante de vigilancia entre las exploraciones. En la mayoría de los casos, esto bastará para proteger la integridad del sistema. Sin embargo, las buenas medidas de seguridad antivirus incorporan exploraciones completas y periódicas del sistema debido a que:

- **La exploración en segundo plano comprueba los archivos mientras se ejecutan**. El explorador VShield busca códigos de virus durante la ejecución de archivos o la lectura de disquetes, mientras que la aplicación VirusScan puede buscar firmas de códigos en los archivos almacenados en el disco duro. Si ejecuta un archivo infectado de forma muy esporádica, puede que el explorador VShield no detecte el virus hasta que despliegue su carga destructiva. Sin embargo, la aplicación VirusScan puede detectar un virus que espera la ocasión para actuar.

- **Los virus son sigilosos**. Si deja accidentalmente un disquete en la unidad al arrancar el equipo, el virus podría cargarse en la memoria antes que el explorador VShield, sobre todo si el explorador no está configurado para explorar disquetes. Una vez en la memoria, un virus puede infectar prácticamente a cualquier programa, incluido el explorador VShield.

- **El explorador VShield necesita tiempo y recursos**. La búsqueda de virus durante la ejecución, copia o almacenamiento de archivos puede retrasar, aunque ligeramente, el arranque de software y otras tareas. Dependiendo de la situación, podría dedicar este tiempo a operaciones de sistema importantes. Aunque las consecuencias son leves, podría verse tentado de desactivar el explorador VShield si necesita toda la potencia disponible para tareas que exijan una gran cantidad de recursos. En ese caso, la realización de operaciones de exploración regulares en períodos de inactividad puede proteger el sistema del ataque de virus sin comprometer su rendimiento.

- **Una buena seguridad es la mejor protección**. En el mundo de redes y conexiones Web en el que se mueven la mayoría de los usuarios informáticos hoy en día, descargar un virus de un origen que probablemente ni siquiera es consciente de haber visitado, es cosa de segundos. Si un problema relacionado con el software desactiva la exploración en segundo plano durante unos segundos, o si no ha configurado una exploración de este tipo para vigilar un punto de entrada vulnerable, su equipo podría terminar infectado. Las operaciones de exploración periódicas a menudo interceptan las infecciones antes de que se extiendan o puedan causar algún daño.

Si se conecta a Internet o descarga archivos con frecuencia, puede que desee programar operaciones de exploración con carácter regular que examinen el sistema a intervalos de tiempo programados con el fin de no tener que estar pendiente de iniciar la aplicación VirusScan. Para ello, la Consola de VirusScan proporciona un conjunto de opciones muy flexible.

Inicio de la aplicación VirusScan

Puede iniciar la aplicación VirusScan en su propia ventana o como parte de una tarea de exploración programada. El método que elija dependerá del tipo de operación de exploración que desee ejecutar. La primera vez que la inicie, se abrirá la ventana de la aplicación con el fin de que el usuario pueda realizar cambios en la configuración. Debe hacer clic en **Explorar ahora** o en **Ejecutar ahora** en un paso diferente para iniciar una operación de exploración real.

Existen cuatro métodos distintos para iniciar la aplicación VirusScan. Los cuatro exigen ejecutar la aplicación desde la línea de comandos. La *Guía del administrador* de VirusScan enumera las opciones de la línea de comandos de este método.

En las siguientes secciones se describe cada método.

Método 1: Mostrar la ventana principal de la aplicación VirusScan

Siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Programas** y, a continuación, McAfee. Después, seleccione **McAfee VirusScan**.

Aparece la ventana principal de VirusScan (figura 5-1).

Figura 5-1. Pantalla McAfee VirusScan Central

Desde aquí, puede:

- **Iniciar la exploración inmediatamente**. Haga clic en **Explorar** para que la aplicación explore el sistema con las últimas opciones de configuración establecidas o con las opciones predeterminadas.

  En la siguiente pantalla (figura 5-2) puede seleccionar el área del ordenador que se va a explorar. Una vez seleccionada, haga clic en Explorar ahora. Complete los pasos de las pantallas siguientes para finalizar la tarea.

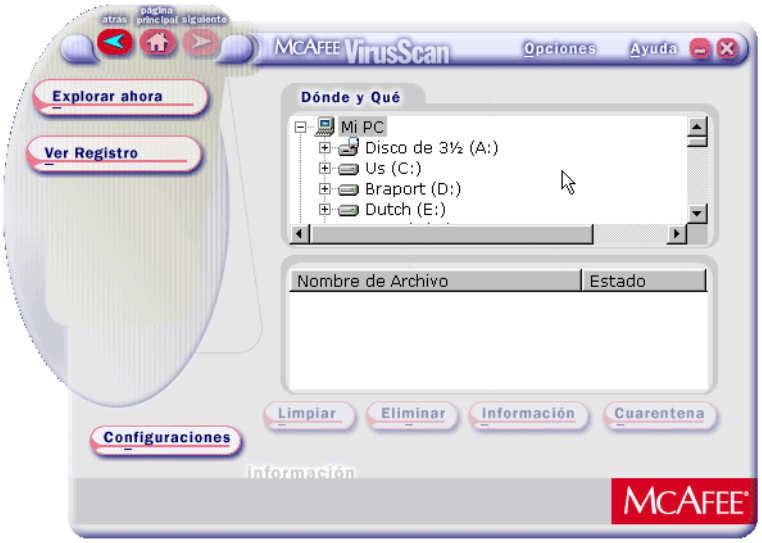

Figura 5-2. Ventana Explorar ahora

- **Ver el registro de actividades de la aplicación VirusScan**. En esta ventana puede ver un registro de las actividades de VirusScan que se han llevado a cabo en el ordenador. También dispone de opciones para borrar o imprimir cualquiera de estos registros de actividades (vea la figura 5-3).

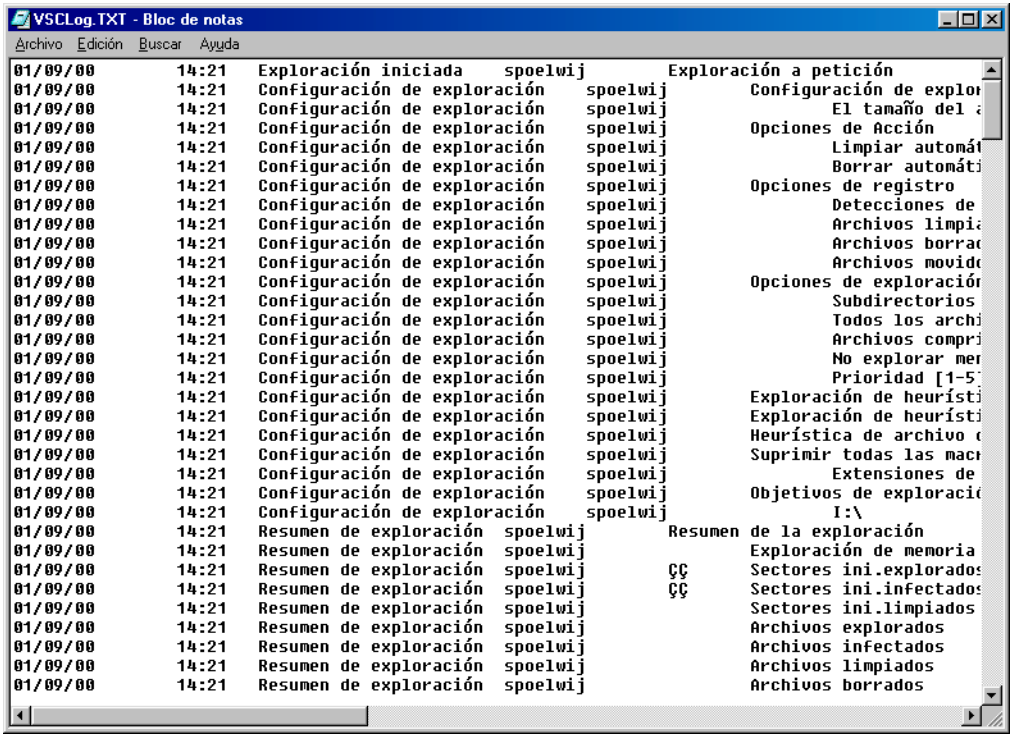

Figura 5-3. Registro de actividades de VirusScan

- **Abra el archivo de ayuda en línea.** Seleccione **Temas de Ayuda** en el menú **Ayuda** para ver una lista de los temas de ayuda de VirusScan. Para ver una descripción contextual de los botones, listas y otros elementos en la ventana de VirusScan, seleccione **¿Qué es esto?** en el menú **Ayuda** y haga clic en el elemento que le interese con el botón izquierdo del ratón después de que el cursor del ratón cambie a ?. Puede ver estos mismos temas de ayuda si hace clic con el botón derecho del ratón en un elemento de la ventana de VirusScan y selecciona **¿Qué es esto?** en el menú que aparece.

2. Defina las opciones. En la ventana principal, el icono Opciones (vea la figura 5-4) le permite acceder a los parámetros de otros componentes de McAfee VirusScan y personalizarlos mediante un menú desplegable (por ejemplo, Safe & Sound y Disco de emergencia).

Figura 5-4. Menú desplegable Opciones

3. Seleccione **X** en el menú **Archivo** para salir de la aplicación.

NOTA: Para obtener más información sobre cualquiera de las funciones, opciones y herramientas a que se puede acceder desde la pantalla principal, consulte la Ayuda en línea.

Método 2: Iniciar una tarea de exploración desde la Consola de VirusScan

---

Siga estos pasos:

1. Haga doble clic en el icono de la Consola de VirusScan en la bandeja del sistema Windows para llevar la ventana de la Consola al primer plano.

   La Consola incluye dos tareas preestablecidas que utilizan la aplicación VirusScan para ejecutarse: Explorar Mi PC y Explorar unidad 'C'.

   Podrá:

- **Iniciar una de las tareas preestablecidas en su configuración predeterminada**. Seleccione una tarea de la lista de tareas y, a continuación, haga clic en  en la barra de herramientas de la Consola. Si la tarea de exploración está configurada para iniciarse de forma automática, la ventana de la aplicación VirusScan se abrirá y la tarea se ejecutará inmediatamente. Si, por el contrario, la tarea no ha sido configurada para iniciarse automáticamente, la ventana se abrirá, pero debe hacer clic en **Explorar ahora** para iniciar la operación.
- **Crear y programar una nueva tarea por su cuenta**. Haga clic en  en la barra de herramientas de la Consola para abrir el cuadro de diálogo Propiedades de tarea. Asigne un nombre a la tarea, seleccione las opciones de seguridad pertinentes, especifique cómo desea que aparezca cuando se ejecute y lo que desea que haga cuando termine. Para establecer las opciones de configuración de la tarea, haga clic en el botón **Configurar** que se encuentra en la parte inferior de la página de propiedades.

2. Haga clic en la ficha Programar para especificar cuando se debe ejecutar la tarea. Active la casilla de verificación **Activar tarea** para prepararla con el fin de ejecutarla a la hora programada.

Configuración de la interfaz de VirusScan en modo Clásico

IMPORTANTE: VirusScan Clásico debe ejecutarse desde el Explorador de Windows o en el menú Ejecutar.

Para que la aplicación VirusScan proteja el sistema, debe indicarle:

- qué debe explorar
- qué desea que haga cuando detecte un virus
- cómo debe avisar cuando detecte un virus
- si debe llevar un registro de las acciones

Las opciones de cada tarea se controlan a través de una serie de páginas de propiedades de la ventana de VirusScan; si desea configurar la aplicación para que realice la tarea, haga clic en cada ficha. Para disponer de más opciones de configuración, cambie a la interfaz de VirusScan en modo Avanzado. Elija **Avanzado** en el menú **Herramientas** en la ventana de VirusScan en modo Clásico.

Puede iniciar una operación de exploración con las opciones elegidas en cualquier lugar, sólo tiene que hacer clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

El archivo de configuración que guarde tendrá un nombre de archivo con extensión .VSC.

Selección de las opciones de Detección de la interfaz de VirusScan Clásico

El software de VirusScan supone inicialmente que desea explorar la unidad C: y todas sus subcarpetas y que le interesa explorar únicamente los archivos susceptibles de contraer un virus (figura 5-5).

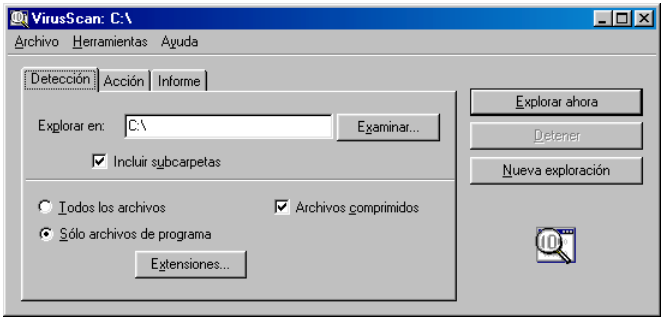

Figura 5-5. Ventana de VirusScan en modo Clásico: página Dónde y qué

Para modificar estas opciones, realice el siguiente procedimiento:

1. Elija el volumen o la carpeta del sistema o de la red en el que desea que el software de VirusScan busque los virus.

   Escriba una ruta para el volumen o carpeta de destino en el cuadro de texto que se proporciona, o haga clic en **Examinar** para abrir el cuadro de diálogo Examinar carpeta (figura 5-6).

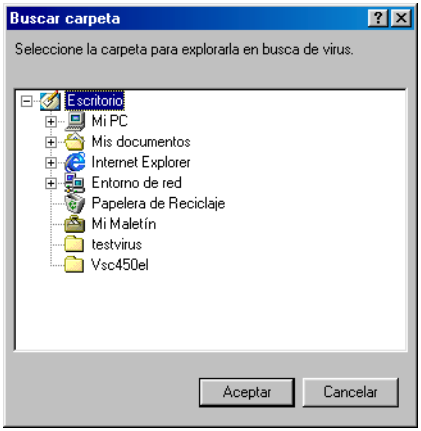

Figura 5-6. Cuadro de diálogo Examinar carpeta

Haga clic en ⊞ para ampliar el listado del elemento que figura en el cuadro de diálogo. Haga clic en ⊟ para cerrar un elemento. Puede seleccionar discos duros, carpetas o archivos como objetivos de exploración, tanto en su sistema como en otros equipos de la red. No puede seleccionar Mi PC, Entorno de red ni volúmenes múltiples como objetivos de exploración de VirusScan en modo Clásico. Para poder hacerlo, debe cambiar al modo Avanzado.

Cuando haya seleccionado el objetivo de exploración, haga clic en **Aceptar** para volver a la ventana de VirusScan en modo Clásico.

2. Active la casilla de verificación **Incluir subcarpetas** para que la aplicación busque virus en las carpetas que pueda haber en el objetivo de exploración.

- **NOTA:** Al elegir **Incluir subcarpetas** la aplicación realiza una exploración sólo en aquellos archivos almacenados en las propias subcarpetas. La aplicación no explorará los archivos almacenados en el directorio raíz de la carpeta designada. Para explorar esos archivos, desactive la casilla de verificación **Incluir subcarpetas**.

---

3. Especifique los tipos de archivos que desee que examine el software de VirusScan. Podrá:

   - **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que el software de VirusScan busque virus en archivos comprimidos y archivos de almacenamiento. Aunque esta opción proporciona mayor protección, la exploración de archivos comprimidos puede aumentar la cantidad de tiempo necesario para las operaciones de exploración.

- **Explorar todos los archivos**. Active la casilla de verificación **Todos los archivos** para que la aplicación explore todos los archivos del destino especificado sea cual sea la extensión.

  - **NOTA:** McAfee VirusScan Software recomienda que seleccione esta opción la primera vez que realice una exploración y periódicamente en futuras ocasiones, para asegurarse de que el sistema no contiene virus. De este modo, puede limitar el ámbito de operaciones de exploración posteriores.

- **Seleccionar los tipos de archivos**. Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea archivos de comandos, macros o códigos binarios. Por tanto, podrá reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, limitándolo a los archivos con mayores probabilidades de ser infectados. Para ello, haga clic en el botón **Sólo archivos de programa**.

  Para ver o designar las extensiones de nombres de archivo que la aplicación examinará, haga clic en **Extensiones**. De este modo se abre el cuadro de diálogo Extensiones de archivos de programa.

4. Haga clic en la ficha Acción para seleccionar otras opciones de VirusScan.

   Para iniciar inmediatamente una operación de exploración sólo con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Acción

Cuando el software de VirusScan detecta un virus, puede reaccionar preguntando qué debe hacer con el archivo infectado o emprendiendo automáticamente la acción que se le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta desea que el software de VirusScan le ofrezca cuando encuentre un virus o qué acciones desea que emprenda automáticamente.

Siga estos pasos:

1. Haga clic en la ficha Acción de la ventana de VirusScan en modo Clásico para ver la página de propiedades correcta (figura 5-7).

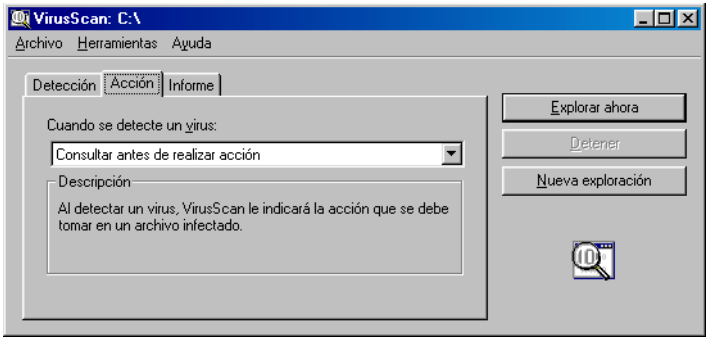

Figura 5-7. Ventana de VirusScan en modo Clásico: página Acción

2. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada inmediatamente debajo de la lista cambiará para mostrar opciones adicionales para cada respuesta. Podrá elegir entre las siguientes opciones:

   - **Consultar al usuario antes de realizar acción.** Seleccione esta respuesta si espera estar delante del ordenador cuando la aplicación VirusScan explore el disco. La aplicación presentará un mensaje de alerta cuando encuentre un virus y le ofrecerá una gama de posibles respuestas.
   - **Mover archivos infectados automáticamente**. Elija esta respuesta si desea que la aplicación mueva los archivos infectados a una carpeta de cuarentena tan pronto como los detecte.

     De forma predeterminada, la aplicación mueve estos archivos a una carpeta denominada Infectados en el directorio de programa de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente o hacer clic en **Examinar** para encontrar una carpeta adecuada en su disco duro.
   - **Limpiar los archivos infectados automáticamente.** Elija esta respuesta para indicar a la aplicación VirusScan que elimine el código de virus del archivo infectado tan pronto como lo detecte. Si la aplicación no puede eliminar el virus, anotará el incidente en el archivo de registro.

- **Eliminar los archivos infectados automáticamente.** Utilice esta opción si desea que la aplicación VirusScan elimine inmediatamente todos los archivos infectados que detecte. Asegúrese de activar la función de informe para poder tener un registro de todos los archivos que la aplicación haya eliminado. Tendrá que recuperar los archivos eliminados de las copias de seguridad. Si la aplicación no puede eliminar el archivo infectado, anotará el incidente en el archivo de registro.
- **Continuar la exploración.** Utilice esta opción sólo si tiene pensado dejar el equipo sin supervisión mientras la aplicación VirusScan comprueba si hay virus. Si también activa la función de generación de informes de la aplicación, el programa registrará los nombres de los virus que detecte y de los archivos infectados para que pueda eliminarlos tan pronto como tenga la oportunidad.

3. Haga clic en la ficha Informe para seleccionar otras opciones de VirusScan.

   Para iniciar inmediatamente una operación de exploración sólo con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Informe

De forma predeterminada, la aplicación VirusScan emite un sonido de alerta cuando detecta un virus. Puede utilizar la página Informe para activar o desactivar esta alerta o para agregar un mensaje de alerta al cuadro de diálogo Se encontraron virus que aparece cuando la aplicación encuentra un archivo infectado. Este mensaje de alerta puede contener cualquier tipo de información, desde una simple advertencia hasta instrucciones sobre el modo de informar del incidente al administrador de la red.

También puede establecer aquí el tamaño y la ubicación del archivo de registro de VirusScan. De forma predeterminada, la aplicación muestra la configuración actual y hace un resumen de todas las acciones que se realizan durante las operaciones de exploración en un archivo de registro llamado VSCLOG.TXT. Es posible hacer que este archivo sea el archivo de registro, o también especificar un archivo de texto existente diferente para que lo utilice la aplicación. La aplicación no creará un archivo de texto nuevo.

Después podrá abrir e imprimir el archivo de registro para examinarlo desde la aplicación VirusScan o desde un editor de texto.

Para seleccionar las opciones de alerta y registro de VirusScan, siga estos pasos:

1. Haga clic en la ficha Informe de la ventana de VirusScan en modo Clásico para ver la página de propiedades correcta (figura 5-8).

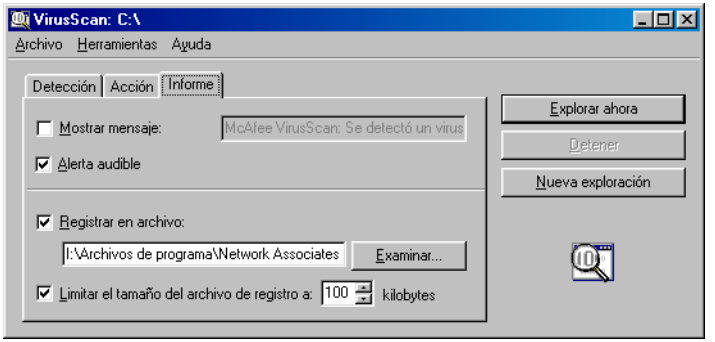

Figura 5-8. Ventana de VirusScan en modo Clásico: página Informe

2. Seleccione los tipos de métodos de alerta que desee que utilice la aplicación VirusScan cuando detecte un virus. Puede hacer que:

   - **Muestre un mensaje personalizado.** Active la casilla de verificación **Mostrar mensaje** y escriba el mensaje que quiere que aparezca en el cuadro de texto. Puede escribir un mensaje de hasta 225 caracteres.

     - **NOTA:** Para que la aplicación VirusScan muestre el mensaje, debe seleccionar **Consultar al usuario antes de realizar acción** como respuesta en la página Acción.

   - **Emita un sonido.** Active la casilla de verificación **Alerta audible.**

3. Active la casilla de verificación **Registrar en archivo**.

   Como opción predeterminada, el software de VirusScan escribe la información de registro en el archivo VSCLOG.TXT en el directorio de programa de VirusScan. Para especificar un archivo de registro distinto de VSCLOG.TXT, escriba un nombre de archivo y una ruta en el cuadro de texto que se proporciona o haga clic en **Examinar** para encontrar un archivo disponible en cualquier lugar de su disco duro o red.

4. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente.

Escriba un valor entre 10 KB y 999 KB. Como opción predeterminada, el software de VirusScan limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño especificado del archivo, el software de VirusScan eliminará el registro existente y comenzará de nuevo desde el punto en que se detuvo.

5. Haga clic en una ficha distinta para cambiar cualquiera de las opciones de VirusScan.

   Para iniciar inmediatamente una operación de exploración con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Configurar la interfaz de VirusScan Avanzado

La interfaz de VirusScan Avanzado ofrece más flexibilidad en las opciones de configuración que la interfaz de VirusScan Clásico, dado que incluye la posibilidad de ejecutar más de una exploración a la vez, de excluir elementos de las exploraciones y de activar la capacidad de detección heurística de la aplicación.

Para que la aplicación VirusScan proteja el sistema, debe indicarle:

- qué debe explorar
- qué desea que haga cuando detecte un virus
- cómo debe avisar cuando detecte un virus
- si debe llevar un registro de las acciones
- qué elementos no desea explorar en busca de virus

Las opciones de cada tarea se controlan a través de una serie de páginas de propiedades de la ventana de VirusScan; si desea configurar la aplicación para que realice la tarea, haga clic en cada ficha. Para realizar la selección en un conjunto más sencillo de opciones de configuración, desplácese a la interfaz de VirusScan Clásico. Elija **Clásico** en el menú **Herramientas** en la ventana de VirusScan Avanzado.

Para proteger las opciones elegidas de cambios no autorizados, seleccione **Protección con contraseña** en el menú **Herramientas** para abrir el cuadro de diálogo.

Puede iniciar una operación de exploración con las opciones elegidas en cualquier lugar, sólo tiene que hacer clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Detección

El software de VirusScan supone inicialmente que desea explorar todos los discos duros del equipo, incluidos los asignados a las unidades de red, y limitar la exploración a los archivos con posibilidades de contraer un virus (figura 5-9).

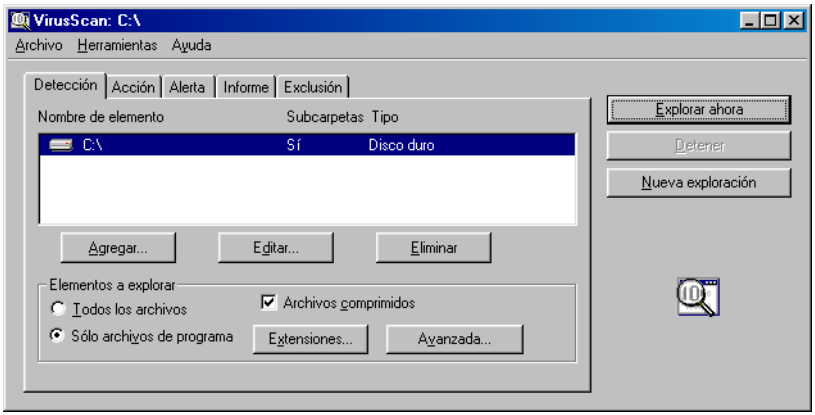

Figura 5-9. Ventana VirusScan Avanzado: página Detección

Para modificar estas opciones y agregar otras, complete los siguientes pasos:

1. Elija las partes del sistema o de la red que desea que explore el software de VirusScan. Podrá:

   - **Agregar objetivos de exploración.** Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar elemento de exploración (figura 5-10).

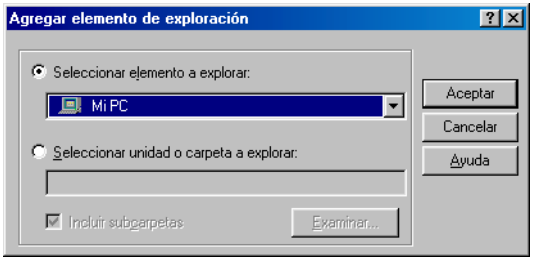

Figura 5-10. Cuadro de diálogo Agregar elemento de exploración

Para explorar todo el equipo o un subgrupo de las unidades del sistema o de la red, haga clic en el botón **Seleccionar elemento a explorar**, a continuación:

a. Seleccione un objetivo que desee explorar en la lista que se proporciona. Podrá elegir entre las siguientes opciones:

   – **Mi PC**. Indica a la aplicación que explore todas las unidades que estén conectadas físicamente al equipo o mediante la asignación de unidades a través del explorador de Windows a una letra de unidad del equipo.

   – **Todos los medios extraíbles**. Indica a la aplicación que explore sólo los disquetes, discos CD-ROM, discos ZIP Iomega o dispositivos de almacenamiento similares que estén conectados físicamente al equipo.

   – **Todos los discos duros**. Indica a la aplicación que explore los discos duros que estén conectados físicamente al equipo.

   – **Todas las unidades de red**. Indica a la aplicación que explore todas las unidades asignadas mediante el explorador de Windows a una letra de unidad del equipo.

b. Cuando haya seleccionado el destino, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Para explorar un disco o una carpeta en concreto del sistema, haga clic en el botón **Seleccionar unidad o carpeta a explorar**, a continuación:

a. Escriba en el cuadro de texto correspondiente la letra de unidad o la ruta de acceso a la carpeta que desea explorar, o haga clic en **Examinar** para buscar el objetivo de exploración en el equipo.

- **NOTA:** No se puede utilizar la notación de la Convención de nomenclatura universal (UNC) para especificar un disco de red como objetivo de exploración de tareas programadas. Si lo hace, obtendrá como resultado un error de ruta no válida. Puede utilizar la notación UNC para especificar objetivos de exploración para operaciones que ejecute directamente con la aplicación VirusScan.

---

b. Active la casilla de verificación **Incluir subcarpetas** para que la aplicación VirusScan busque también virus en las carpetas que pueda haber en el objetivo de exploración.

- **NOTA:** Al elegir **Incluir subcarpetas** la aplicación realiza una exploración sólo en aquellos archivos almacenados en las propias subcarpetas. La aplicación no explorará los archivos almacenados en el directorio raíz de la carpeta designada. Para explorar esos archivos, desactive la casilla de verificación **Incluir subcarpetas**.

---

c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Cambiar los objetivos de exploración.** Seleccione uno de los objetivos de exploración de la lista y haga clic en **Editar** para abrir el cuadro de diálogo Editar elemento de exploración (figura 5-11).

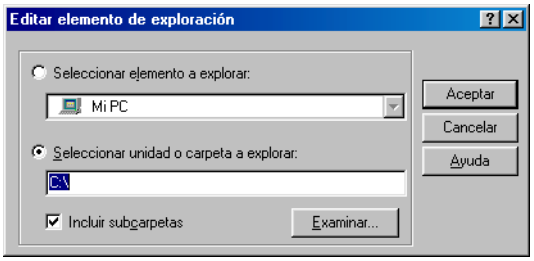

Figura 5-11. Cuadro de diálogo Editar elemento de exploración

En el cuadro de diálogo aparecerá seleccionado el objetivo de exploración existente. Seleccione o escriba un nuevo objetivo de exploración y, a continuación, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Eliminar objetivos de exploración.** Seleccione uno de los objetivos de exploración detallados y haga clic en **Eliminar** para eliminarlo.

2. Especifique los tipos de archivos que desea que examine la aplicación VirusScan. Podrá:

   - **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que la aplicación VirusScan busque virus en archivos comprimidos y archivos de almacenamiento. Aunque esta opción proporciona mayor protección, la exploración de archivos comprimidos puede aumentar la cantidad de tiempo necesario para las operaciones de exploración.

   - **Explorar todos los archivos**. Active la casilla de verificación **Todos los archivos** para que la aplicación explore todos los archivos del destino especificado sea cual sea la extensión.

     - **NOTA:** McAfee VirusScan Software recomienda que seleccione esta opción la primera vez que realice una exploración y periódicamente en futuras ocasiones, para asegurarse de que el sistema no contiene virus. De este modo, puede limitar el ámbito de operaciones de exploración posteriores.

   - **Seleccionar los tipos de archivos**. Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea archivos de comandos, macros o códigos binarios. Por tanto, podrá reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, limitándolo a los archivos con mayores probabilidades de ser infectados. Para ello, haga clic en el botón **Sólo archivos de programa**.

     Para ver o designar las extensiones de nombres de archivo que la aplicación examinará, haga clic en **Extensiones**. De este modo se abre el cuadro de diálogo Extensiones de archivos de programa.

3. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración (figura 5-12).

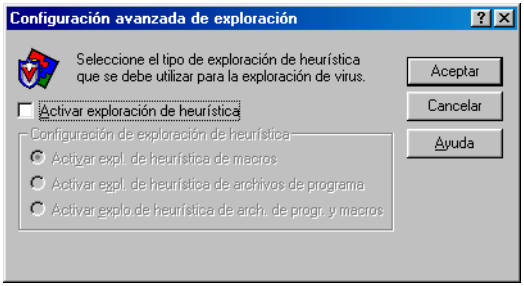

Figura 5-12. Cuadro de diálogo Configuración avanzada de exploración

La tecnología de exploración heurística permite a la aplicación VirusScan reconocer nuevos virus basándose en su parecido a virus similares que el módulo ya conoce. Para hacerlo, la aplicación busca determinadas características "tipo virus" en los archivos especificados para explorar. La presencia de una cantidad suficiente de estas características en un archivo lleva a la aplicación a identificarlo como posiblemente infectado con un nuevo virus o con uno que aún no ha sido identificado.

Puesto que la aplicación busca simultáneamente características en el archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas de infección. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

La aplicación VirusScan se inicia sin ninguna opción de exploración heurística activa. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que desee que la aplicación VirusScan utilice. Podrá elegir entre las siguientes opciones:

   – **Activar expl. de heurística de macros**. Elija esta opción para que la aplicación identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que incluyan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. La aplicación identificará las coincidencias totales con el nombre del virus correspondiente. Cuando las firmas del código recuerden a virus existentes, dicha aplicación indicará que ha encontrado un posible virus de macro.

– **Activar expl. de heurística de arch. de programa.** Elija esta opción para que la aplicación VirusScan localice nuevos virus en archivos de programa examinando sus características y comparándolas con una lista de características de virus conocidos. La aplicación identificará los archivos que tengan un número suficiente de estas características como posibles virus.

– **Activar expl. de heurística de arch. de programa y macros.** Elija esta opción para que la aplicación utilice ambos tipos de exploración heurística. McAfee VirusScan Software aconseja el uso de esta opción para obtener una protección antivirus total.

• **NOTA:** La aplicación utilizará técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide examinar **Todos los archivos**, utilizará una exploración heurística para todos los tipos de archivos.

---

c. Haga clic en **Aceptar** para guardar la configuración y volver al cuadro de diálogo Propiedades de VShield.

4. Haga clic en la ficha Acción para seleccionar opciones adicionales de la aplicación VirusScan.

   Para iniciar inmediatamente una operación de exploración sólo con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Acción

Cuando el software de VirusScan detecta un virus, puede reaccionar preguntando qué debe hacer con el archivo infectado o emprendiendo automáticamente la acción que se le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta desea que el software de VirusScan le ofrezca cuando encuentre un virus o qué acciones desea que emprenda automáticamente.

Siga estos pasos:

1. Haga clic en la ficha Acción de la ventana de VirusScan en modo Avanzado para ver la página de propiedades correcta (figura 5-13).

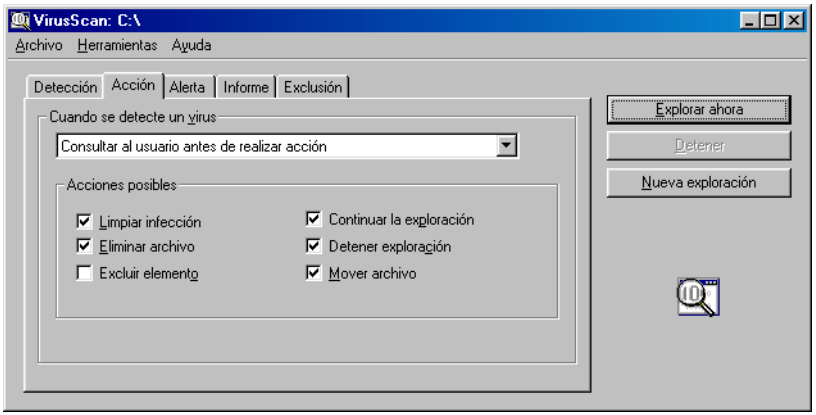

Figura 5-13. VirusScan Avanzado: página Acción

2. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada inmediatamente debajo de la lista cambiará para mostrar opciones adicionales para cada respuesta. Podrá elegir entre las siguientes opciones:

   - **Consultar al usuario antes de realizar acción.** Elija esta respuesta si espera estar trabajando con el equipo cuando la aplicación VirusScan explore el disco. El programa presentará mensajes de alerta cuando encuentre un virus y le ofrecerá una gama de posibles respuestas.

     Cada casilla de verificación que se active en la página Acción hace que aparezca un botón en el mensaje de alerta que la aplicación muestra cuando encuentra un virus. Por ejemplo, al seleccionar **Eliminar archivo**, aparecerá el botón **Eliminar** en el mensaje de alerta.

     Puede seleccionar una de las siguientes opciones:

     – **Limpiar infección**. Esta opción indica a la aplicación que intente eliminar el código de virus del archivo infectado. Si la función de elaboración de informes está activada, grabará un suceso de registro cada vez que limpie o no pueda limpiar un archivo infectado.

     – **Eliminar archivo**. Esta opción indica a la aplicación que elimine inmediatamente el archivo infectado.

  - **Excluir elemento**. Esta opción indica a la aplicación que ignore el archivo durante las operaciones de exploración posteriores. Es la única opción cuya selección no está predeterminada.
  - **Continuar la exploración**. Esta opción indica a la aplicación que continúe con la exploración, pero que no emprenda ninguna otra acción. Si las opciones de generación de informes están activadas, la aplicación incluirá el incidente en su archivo de registro.
  - **Detener exploración**. Esta opción indica a la aplicación que detenga inmediatamente la operación de exploración. Para continuar, debe hacer clic en **Explorar ahora** para reiniciar la operación.
  - **Mover archivo**. Esta opción indica a la aplicación que desplace el archivo infectado a una carpeta de cuarentena. Los mensajes de alerta mostrarán un botón **Mover archivo a** que el usuario puede utilizar para buscar una carpeta de cuarentena.

- **Mover archivos infectados automáticamente**. Elija esta respuesta para que la aplicación mueva los archivos infectados a la carpeta de cuarentena.

  De forma predeterminada, la aplicación mueve estos archivos a una carpeta denominada \Infectados en el directorio de programa de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente o hacer clic en **Examinar** para encontrar una carpeta adecuada en su disco duro.

- **Limpiar los archivos infectados automáticamente**. Elija esta respuesta para indicar a la aplicación que elimine el código de virus del archivo infectado tan pronto como lo detecte. Si la aplicación no puede eliminar el virus, anotará el incidente en el archivo de registro.

- **Eliminar los archivos infectados automáticamente**. Elija esta opción si desea que la aplicación elimine inmediatamente todos los archivos infectados que detecte. Asegúrese de activar la función de generación de informe para poder tener un registro de todos los archivos que la aplicación haya eliminado. Tendrá que recuperar los archivos eliminados de las copias de seguridad. Si la aplicación no puede eliminar el archivo infectado, anotará el incidente en el archivo de registro.

- **Continuar la exploración**. Utilice esta opción sólo si prevé dejar el equipo sin atención mientras la aplicación comprueba si hay virus. Si también activa la función de generación de informes, la aplicación registrará los nombres de los virus que encuentre y de los archivos infectados para que los elimine tan pronto como tenga la oportunidad.

3. Haga clic en la ficha Alerta para seleccionar otras opciones de VirusScan.

   Para iniciar inmediatamente una operación de exploración sólo con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Alerta

Una vez configurada la aplicación VirusScan con las opciones de respuesta que desee, puede dejar que busque y elimine automáticamente virus del sistema, conforme los vaya encontrando, sin apenas intervención posterior. Para que la aplicación le informe automáticamente de que ha encontrado un virus con el fin de tomar las medidas apropiadas, es necesario configurarlo para que le envíe el correspondiente mensaje de alerta.

Siga estos pasos:

1. Haga clic en la ficha Alerta de la ventana de VirusScan en modo Avanzado para ver la página de propiedades correcta (figura 5-14).

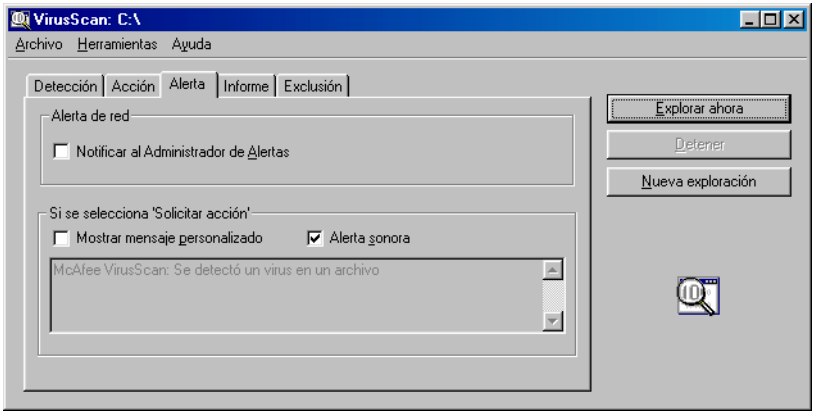

Figura 5-14. VirusScan Avanzado: página Alerta

2. Active la casilla de verificación **Notificar al Administrador de alertas** para que la aplicación VirusScan envíe mensajes de alerta al Administrador de alertas para su distribución.

   El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que la aplicación VirusScan envíe satisfactoriamente estos mensajes de alerta, debe configurar la utilidad de configuración de cliente del Administrador de alertas.

   Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

   - **NOTA:** Si se desactiva esta casilla de verificación, la aplicación VirusScan no enviará ningún mensaje de alerta mediante el Administrador de alertas; sin embargo, esto no afecta a otros mensajes de alerta configurados en esta página de propiedades.

3. Active la casilla de verificación **Alerta sonora** para que la aplicación emita un sonido cuando encuentre un archivo infectado.

   Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**. La aplicación hará sonar un sonido estándar de alerta del sistema o hará que el equipo ejecute el archivo .WAV que se haya definido previamente.

4. Active la casilla de verificación **Mostrar mensaje personalizado** para que la aplicación agregue un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

   Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

5. Escriba el mensaje que desee que muestre la aplicación en el cuadro de texto proporcionado. Puede escribir 250 caracteres como máximo.

6. Haga clic en la ficha Informe para seleccionar otras opciones de configuración de VirusScan.

   Para iniciar inmediatamente una operación de exploración sólo con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Informe

La aplicación VirusScan enumera la configuración actual y resume todas las acciones que emprende durante las operaciones de exploración en un archivo de registro denominado VSCLOG.TXT. Puede hacer que la aplicación escriba su registro en ese archivo o puede utilizar cualquier editor de textos para crear un archivo de texto con el fin de que lo utilice la aplicación. Después podrá abrir e imprimir el archivo de registro para examinarlo posteriormente desde la aplicación o desde el editor de texto.

El archivo VSCLOG.TXT puede ser una herramienta muy importante para efectuar un seguimiento de la actividad de los virus en su sistema y tomar nota de los parámetros de configuración utilizados para detectar y responder a las infecciones que encuentre la aplicación VirusScan. También puede utilizar los informes de incidentes que se registran en el archivo para determinar qué archivos tiene que reemplazar a partir de las copias de seguridad, cuáles debe examinar de los que se encuentran en el área de cuarentena y cuáles debe eliminar del equipo. Utilice la página de propiedades Informes para determinar qué información debe incluir la aplicación en su archivo de registro.

Para ver el contenido del archivo de registro, elija **Ver registros de actividades** en el menú **Archivo** en la ventana de la aplicación VirusScan.

Para hacer que el software de VirusScan registre sus acciones en un archivo de registro, siga los siguientes pasos:

1. Haga clic en la ficha Informe de la ventana de VirusScan en modo Avanzado para ver la página de propiedades correcta (figura 5-15).

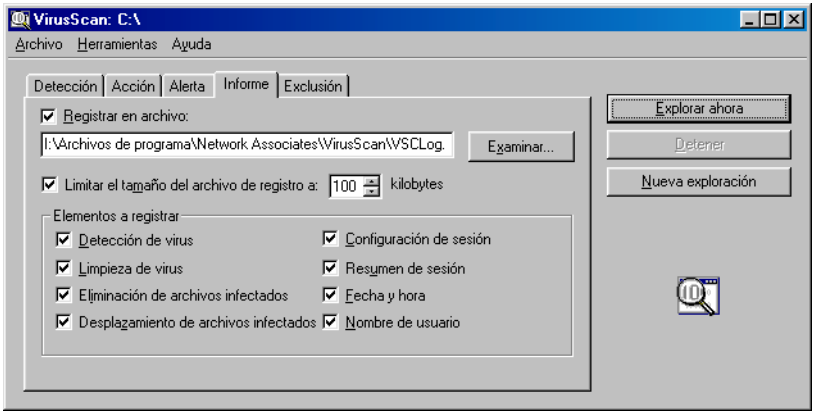

Figura 5-15. VirusScan Avanzado: página Informe

2. Active la casilla de verificación **Registrar en archivo**.

   Como opción predeterminada, la aplicación VirusScan escribe la información de registro en el archivo VSCLOG.TXT, en el directorio de programa de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente, o hacer clic en **Examinar** para encontrar un archivo adecuado en su disco duro o en la red. Puede utilizar un archivo diferente, pero debe existir el archivo de texto. La aplicación no creará ningún archivo nuevo.

3. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente. Si no activa esta casilla de verificación, el tamaño del archivo de registro puede aumentar tanto como el espacio en disco lo permita.

   Escriba un valor entre 10 KB y 999 KB. Como opción predeterminada, la aplicación limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, la aplicación eliminará el registro existente y comenzará de nuevo desde el punto en el que se quedó.

4. Active las casillas de verificación que correspondan a la información que desea que la aplicación incluya en el archivo de registro. Cada casilla de verificación que se selecciona aquí hace que la aplicación registre esa información, normalmente cuando la exploración finaliza, o cuando el usuario apaga el sistema:

- **Detección de virus**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación encuentre durante cada operación de exploración. Desactive la casilla de verificación para no incluir esta información en el archivo de registro.
- **Limpieza de virus**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación limpie o intente limpiar durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Eliminación de archivos infectados**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación elimine durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Desplazamiento de archivos infectados**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación mueva a una carpeta de cuarentena durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Configuración de sesión**. Active esta casilla de verificación para que el archivo de registro recoja las opciones de configuración utilizadas por la aplicación durante cada operación de configuración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Resumen de sesión**. Active esta casilla de verificación para que el archivo de registro haga un resumen de las acciones que la aplicación realizó durante cada operación de exploración. El registro incluirá:
  - Número de archivos que la aplicación ha examinado.
  - Número de archivos infectados que la aplicación ha limpiado.
  - Número de archivos infectados que la aplicación ha eliminado.
  - Número de archivos infectados que la aplicación ha movido a una carpeta de cuarentena.
  - Las opciones de configuración de la aplicación.

  Desactive la casilla de verificación para no incluir esta información en el archivo de registro.

- **Fecha y hora**. Active esta casilla de verificación para que se escriban en el archivo de registro la fecha y la hora a la que el software comenzó la operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Nombre de usuario**. Active esta casilla de verificación para que el archivo de registro recoja el nombre de usuario registrado en la estación de trabajo cuando el software inicie cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

5. Haga clic en la ficha Exclusión para seleccionar otras opciones de VirusScan.

   Para iniciar inmediatamente una operación de exploración sólo con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Selección de las opciones de Exclusión

Muchos de los archivos que contiene el equipo no pueden infectarse. Las operaciones de exploración que examinan esos archivos pueden tardar mucho tiempo y producen escasos resultados. Puede acelerar las operaciones de exploración indicando a la aplicación VirusScan que sólo examine los tipos de archivos que tienen probabilidades de estar infectados o indicarle que excluya archivos y carpetas completas que sabe que no se infectarán.

Una vez que haya explorado exhaustivamente el sistema, puede excluir los archivos y carpetas que no cambian o aquellos que no suelen ser vulnerables a infecciones de virus. Además puede confiar en el explorador VShield para disponer de protección entre las operaciones de exploración programadas. Sin embargo, la realización de operaciones periódicas de exploración que examinen todas las zonas del equipo constituye la mejor defensa contra los virus.

Para evitar que la exploración examine los archivos no se infectan, puede identificar los discos, carpetas o archivos individuales que desea excluir de las operaciones de exploración en una lista de exclusión. De forma predeterminada, la aplicación VirusScan no explora la Papelera de reciclaje, ya que Windows no ejecutará los elementos que se hayan almacenado en dicho lugar. Por lo tanto, dichos elementos aparecerán en la lista de exclusión la primera vez que se abra la ventana.

Cada registro de la lista de exclusión muestra la ruta del elemento, especifica si la aplicación también excluirá cualquier carpeta anidada del objetivo y explica si la aplicación excluirá el elemento al explorar los archivos, cuando explore el sector de arranque del disco duro o en ambos casos.

Puede excluir de forma predeterminada hasta 100 objetivos únicos de exploración. Para cambiar este número, abra el panel de control de VirusScan, haga clic en la ficha Componentes y, a continuación, inserte una nueva cifra en el cuadro de texto **Número máximo de elementos excluidos**.

Para excluir archivos o carpetas de las actividades de exploración, siga estos pasos:

1. Haga clic en la ficha Exclusión de la ventana de VirusScan en modo Avanzado para ver la página de propiedades correcta (figura 5-16).

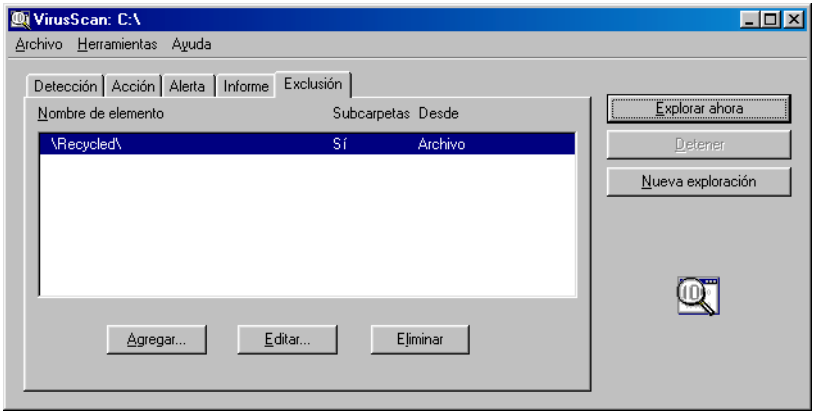

Figura 5-16. Ventana VirusScan Avanzado: página Exclusión

2. Especifique los elementos que desea excluir. Podrá:

   - **Agregar archivos, carpetas o volúmenes a la lista de exclusión.** Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar elemento de exclusión (figura 5-17).

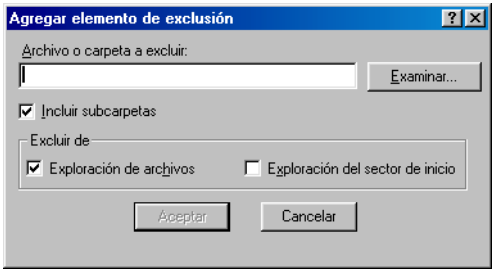

Figura 5-17. Cuadro de diálogo Agregar elemento de exclusión

A continuación, siga los siguientes pasos para agregar elementos a la lista:

a. Escriba una ruta en una carpeta o un nombre de archivo en el cuadro de texto que se proporciona o haga clic en **Examinar** para buscar el elemento que desea que la aplicación excluya.

- **NOTA:** Si ha elegido mover los archivos infectados automáticamente a una carpeta de cuarentena, la aplicación excluirá esa carpeta de las operaciones de exploración.

---

b. Active la casilla de verificación **Incluir subcarpetas** para indicar a la aplicación que ignore los archivos almacenados en cualquier subcarpeta de la carpeta especificada en el paso a.

- **NOTA:** Al elegir **Incluir subcarpetas** la aplicación ignorará sólo aquellos archivos almacenados en las propias subcarpetas. La aplicación todavía explorará los archivos almacenados en el directorio raíz de la carpeta que indique. Para excluir los archivos del directorio raíz, desactive la casilla de verificación **Incluir subcarpetas**.

---

c. Active la casilla de verificación **Exploración de archivos** para excluir el elemento especificado en el primer paso de las operaciones de exploración en las que la aplicación busca virus que infecten archivos. Normalmente, estos virus aparecen en archivos que forman parte de las partes visibles del disco duro.

d. Active la casilla de verificación **Exploración del sector de inicio** para excluir el elemento especificado en el primer paso de las operaciones de exploración en las que la aplicación busca virus en el sector de arranque.

Estos virus normalmente aparecen en la memoria o en los archivos que residen en el sector de arranque o el registro de arranque principal del disco duro. Utilice esta opción para excluir archivos del sistema, como COMMAND.COM, de las operaciones de exploración.

+ **ADVERTENCIA:** McAfee VirusScan aconseja *no* excluir los archivos de sistema de las operaciones de exploración.

e. Repita los pasos del a. al d. hasta que haya incluido en la lista todos los archivos y carpetas que no desee explorar.

- **Modificar la lista de exclusión.** Para cambiar la configuración de un elemento de exclusión, selecciónelo en la lista de exclusiones y, seguidamente, haga clic en **Editar** para abrir el cuadro de diálogo Editar elemento de exclusión. Efectúe los cambios necesarios y haga clic en **Aceptar** para cerrar el cuadro de diálogo.
- **Eliminar un elemento de la lista.** Para eliminar un elemento de exclusión, selecciónelo en la lista y haga clic en **Eliminar**. Esto significa que la aplicación VirusScan *explorará* este archivo o carpeta durante la siguiente operación de exploración.

3. Haga clic en una ficha distinta para cambiar cualquiera de las opciones de VirusScan.

   Para iniciar inmediatamente una operación de exploración con las opciones seleccionadas, haga clic en **Explorar ahora**. Para guardar los cambios como opciones de exploración predeterminadas, seleccione **Guardar como predeterminado** en el menú **Archivo** o haga clic en **Nueva exploración**. Para guardar las opciones en un nuevo archivo, seleccione **Guardar configuración** en el menú **Archivo**, asigne un nombre al archivo en el cuadro de diálogo que aparece y haga clic en **Guardar**.

Activación de la protección con contraseña

El software de VirusScan le permite establecer una contraseña para proteger los valores de configuración seleccionados en cada página de propiedades frente a cambios no autorizados. Esta función es muy útil para administradores de sistema que deseen impedir que los usuarios manipulen sus medidas de seguridad mediante el cambio de las opciones de configuración de VirusScan. Utilice la página Seguridad para bloquear las configuraciones realizadas.

Para activar la protección con contraseña para VirusScan Avanzado, realice los siguientes pasos:

1. Seleccione **Proteger mediante contraseña** en el menú **Herramientas** de la ventana de VirusScan Avanzado para abrir el cuadro de diálogo de Protección con contraseña (figura 5-18).

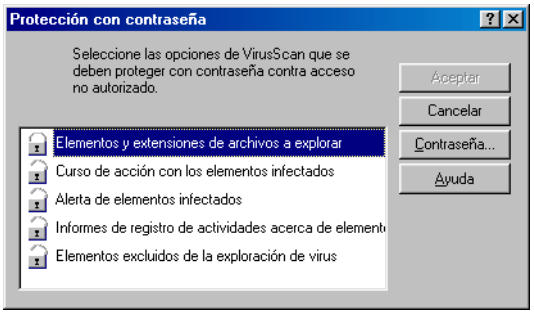

Figura 5-18. Cuadro de diálogo Protección con contraseña

2. Seleccione la configuración que desee proteger en la lista que aparece.

   Puede proteger una o todas las páginas de propiedades de VirusScan. Las páginas de propiedades protegidas se indican mediante un icono de candado cerrado en la lista de seguridad que se muestra. Para eliminar la protección de una página de propiedades, haga clic en el icono de candado cerrado para abrirlo.

3. Haga clic en **Contraseña** para abrir el cuadro de diálogo Especificar contraseña (figura 5-19).

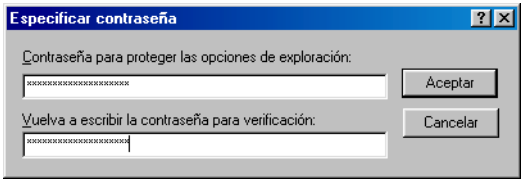

Figura 5-19. Cuadro de diálogo Especificar contraseña

   a. Escriba una contraseña en el primer cuadro de texto que se muestra y, después, vuelva a escribirla en el cuadro de texto que hay debajo del primero para confirmar la selección.

   b. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Especificar contraseña.

4. Haga clic en **Aceptar** para volver a la ventana de VirusScan Avanzado.

Creación y configuración de tareas programadas 6

¿Qué hace la Consola de VirusScan?

La Consola de VirusScan tiene como función principal ejecutar las operaciones de exploración y otras tareas en las fechas y a las horas que elija, o con la periodicidad que fije. Puede utilizar la Consola para ejecutar una operación de exploración en su ausencia, cuando menos interfiera en su trabajo, como parte de una serie de tareas automatizadas o de cualquier otra forma que le convenga. La Consola de VirusScan puede convertirse en la piedra angular de su estrategia de seguridad antivirus si la configura para ejecutar varias tareas relacionadas o entrelazadas que proporcionan cobertura en los períodos de inactividad o de no uso del equipo. Por ejemplo, las tareas independientes en ciclos individuales pueden explorar diferentes partes del sistema o proporcionar cobertura a eventos de trabajo periódicos y predecibles.

La Consola también permite iniciar y detener varias otras operaciones importantes de VirusScan, incluidas las sesiones de exploración de VShield. Puede conectarse al sitio Web de McAfee AVERT Labs para obtener información acerca de virus, abrir y ver archivos de registro, y copiar y pegar definiciones de tareas en la ventana de la Consola.

¿Por qué se programan las operaciones de exploración?

Aunque el software de VirusScan incluye componentes que buscan virus continuamente o que le permiten explorar su sistema cuando desee, debería programar operaciones periódicas de exploración y otras actividades de software para:

- **Establecer bases periódicas para su sistema**. Si desea realizar un seguimiento del sistema o de la red para buscar actividades de virus recurrentes, programe una exploración completa del sistema a intervalos periódicos. Las opciones de generación de informe del software de VirusScan pueden proporcionarle un informe completo sobre el número, el tipo, el tamaño y otras características de cualquier virus que encuentre.

- **Complementar o sustituir la exploración automática o de acceso**. McAfee VirusScan Software recomienda utilizar el software de VShield para explorar constantemente el sistema en busca de virus, pero si su entorno no le permite usarlo o si tiene otros problemas relacionados con el rendimiento del sistema, deberá programar operaciones de exploración frecuentes para evitar infecciones. Incluso si utiliza el software de VShield, la programación de operaciones de exploración periódicas y completas del sistema reducirá la posibilidad de que haya archivos infectados que permanezcan sin detectar.
- **Alternar las operaciones de exploración**. La programación de las operaciones de exploración permite elegir distintas operaciones con diferente finalidad o para momentos diferentes. Si, por ejemplo, desea utilizar el software de VShield para explorar continuamente el sistema y realizar una exploración menos frecuente de las unidades de red asignadas, puede programar una tarea de exploración con esta finalidad.

La Consola incluye un conjunto predeterminado de tareas ya configuradas, pero aún no programadas. Este conjunto incluye tareas que inician el explorador VShield al iniciar el equipo, que realizan una exploración de todas las unidades incluidas en el grupo de Mi PC, que exploran la unidad C: y que actualizan los archivos de datos del software de VirusScan, así como los componentes de programa. Puede activar cualquier tarea predeterminada o crear sus propias tareas según sus hábitos de trabajo.

Inicio de la Consola de VirusScan

Es necesario que la Consola de VirusScan esté funcionando para poder ejecutar cualquier tarea que haya programado. McAfee VirusScan Software recomienda configurar la Consola para que se inicie automáticamente, tan pronto como inicie el equipo.

Para hacerlo, siga los siguientes pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.
2. Localice y haga doble clic en el panel de control de VirusScan 

para abrirlo.

3. Haga clic en la ficha Componentes (Figura 6-1).

Figura 6-1. Panel de control de VirusScan: página Componentes

4. Active la casilla de verificación **Cargar al inicio** en el área de la Consola de VirusScan en la página Componentes.

5. Haga clic en **Aceptar** para cerrar el panel de control.

Cuando vuelva a reiniciar el equipo, también se iniciará la Consola, pero permanecerá minimizada en un icono en la bandeja del sistema de Windows. Para que la ventana de la Consola aparezca en primer plano, haga doble clic en el icono (Figura 6-2).

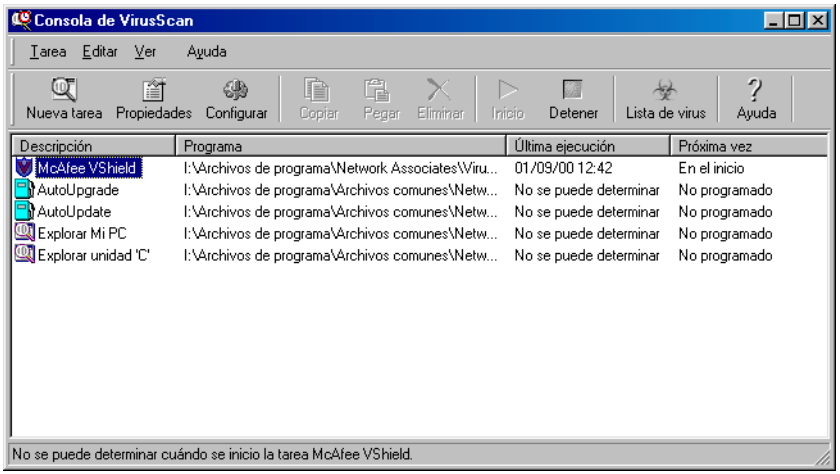

Figura 6-2. Ventana de la Consola de VirusScan

Si el icono no aparece en la bandeja del sistema:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Programas** y, a continuación, **McAfee**.
2. Seleccione la **Consola de VirusScan** para que aparezca la ventana de la Consola.

Una vez que pueda ver la ventana de la Consola, también podrá asegurar que se cargue automáticamente al iniciar si selecciona **Cargar al inicio** en el menú **Ver**.

La ventana de la Consola muestra inicialmente una lista de tareas predeterminadas que se incluyen con la Consola, preconfiguradas y listas para ejecutarse. Una "tarea" es un conjunto de instrucciones necesarias para ejecutar un programa determinado, en una configuración definida y en el momento elegido. Junto con el nombre de cada tarea, la ventana de la Consola muestra la ruta y el nombre de archivo del programa que dicha tarea ejecutará en el tiempo establecido. Las tareas que cree siempre ejecutarán la aplicación VirusScan. Las tareas creadas más recientemente aparecerán en la parte inferior de la ventana de la Consola. La Consola también muestra la hora y la fecha en las que se ejecutó dicha tarea, así como la fecha y la hora en las que tendrá lugar la siguiente.

La barra de herramientas que aparece en la parte superior de la ventana de la Consola proporciona un rápido acceso a los comandos más habituales del programa. Para que dicha barra de herramientas muestre únicamente los botones de los comandos, haga clic en **Ver**, seleccione **Barra de herramientas**, y, a continuación, **Botones estándar**.

Para agregar texto a los botones, haga clic en **Ver**, seleccione **Barra de herramientas** y, a continuación, **Etiquetas**. Es posible tener activas ambas opciones al mismo tiempo: una marca de verificación al lado del elemento de menú indica la vista que se encuentra activa. Encontrará la mayor parte de los mismos comandos de la barra de herramientas en la parte superior de la ventana de la Consola y en los menús de acceso directo que aparecen al hacer clic con el botón derecho del ratón en una de las tareas que aparece en la lista.

El número de tareas incluidas en la lista aparece en la barra de estado de la parte inferior de la ventana de la Consola. Al seleccionar una de las tareas que aparecen en la lista, la barra de estado indica cuándo se ejecutó por última vez dicha tarea. La barra de estado muestra también una breve descripción de cada botón de la barra de herramientas cuando se pasa el cursor del ratón sobre los mismos. Elija **Barra de título** o **Barra de estado** en el menú **Ver** para mostrar u ocultar cada elemento de la ventana.

Utilización de la ventana de la Consola

Desde la ventana de la Consola, podrá:

- **Crear una nueva tarea.** Elija **Nueva tarea** en el menú **Tarea**, o haga clic en  en la barra de herramientas de la Consola. Aparecerá el cuadro de diálogo Propiedades de tarea.
- **Programar y activar tareas.** Seleccione una de las tareas que aparecen en la lista de la ventana de la Consola y, a continuación, seleccione **Propiedades** en el menú **Tarea** o haga clic en  en la barra de herramientas de la Consola. Aparecerá el cuadro de diálogo Propiedades de tarea.
- **Configurar la tarea.** Seleccione una de las tareas que aparecen en la ventana de la Consola y, a continuación, haga clic en  en la barra de herramientas de la Consola para mostrar la página de propiedades del componente de VirusScan que ejecutará la tarea. El aspecto de esta página de propiedades dependerá del componente de VirusScan que se ejecute.
- **Copiar una tarea.** Seleccione una de las tareas que aparecen en la lista de la ventana de la Consola y, a continuación, seleccione **Copiar** en el menú **Edición** o haga clic en  en la barra de herramientas de la Consola. De este modo, la tarea se copiará en el portapapeles de Windows. A continuación, haga clic en la ventana de la Consola y elija **Pegar** en el menú **Edición** o haga clic en  en la barra de herramientas de la Consola para pegar la tarea copiada a la lista de la Consola. Utilice esta función para copiar opciones de tarea con el fin de utilizarlas como plantillas para tareas similares.
- **Eliminar una tarea.** Seleccione una de las tareas que aparecen en la lista de la ventana de la Consola y, a continuación, seleccione **Eliminar** en el menú **Tarea** o haga clic en  en la barra de herramientas de la Consola.

  - **NOTA**: Sólo puede eliminar aquellas tareas que haya creado. No podrá eliminar ninguna de las tareas predeterminadas que se incluyen con la Consola. Sin embargo, puede desactivar cualquier tarea predeterminada que no desee ejecutar.

- **Iniciar una tarea.** Seleccione una de las tareas que aparecen en la lista de la ventana de la Consola y, a continuación, elija **Inicio** en el menú **Tarea**, o haga clic en  en la barra de herramientas de la Consola. La tarea seleccionada se iniciará inmediatamente y se ejecutará con las opciones que haya elegido. Para activar el explorador VShield, seleccione la tarea VShield y, a continuación, elija **Activar** en el menú **Tarea**. Para iniciar explorador y cargarlo en la memoria, seleccione la tarea VSield y, a continuación, haga clic en  en la barra de herramientas de la Consola.

- **Detener una tarea.** Seleccione una de las tareas que aparecen en la lista de la ventana de la Consola y, a continuación, seleccione **Detener ahora** en el menú **Tarea**, o haga clic en  en la barra de herramientas de la Consola. Para detener el explorador VShield, seleccione la tarea VShield y, a continuación, haga clic en  en la barra de herramientas de la Consola o seleccione **Desactivar** en el menú **Tarea**.

- **Conectarse con la Biblioteca de información sobre virus.** Seleccione **Lista de virus** en el menú **Ver**, o haga clic en  en la barra de herramientas de la Consola. La Consola iniciará la aplicación del visualizador que desee y le conectará con el sitio Web de AVERT.

  - **NOTA:** Para conectarse con la Biblioteca de información sobre virus, el equipo deberá disponer de una conexión a Internet y del software de un visualizador de Web.

- **Abra el archivo de ayuda en línea.** Elija **Temas de Ayuda** en el menú **Ayuda** o haga clic en  en la barra de herramientas de la Consola para ver una lista con los temas de ayuda del software de VirusScan. También puede hacer clic con el botón derecho del ratón en la mayoría de los botones de cuadro de diálogo, listas, menús y otros elementos para ver los temas de ayuda contextual. Seleccione el elemento **¿Qué es esto?** que aparece al hacer clic con el botón derecho del ratón en un cuadro de diálogo para ver los temas de ayuda.

- **Ver un registro de actividades.** Seleccione una de las tareas que aparecen en la lista de la ventana de la Consola y, a continuación, elija **Ver registro de actividades** en el menú **Tarea**. No todas las tareas tienen un archivo de registro asociado, pero el software de VirusScan lo abrirá para aquellas que lo tengan en una ventana del Bloc de notas. Puede imprimir, modificar, copiar o tratar este archivo como lo haría con cualquier archivo de texto normal.

- **Proteger las tareas con una contraseña**. Seleccione cualquiera de las tareas que aparecen en la lista de la ventana de la Consola con excepción de la tarea VShield y, a continuación, elija **Tarea de protección de contraseña** en el menú **Tarea** para abrir el cuadro de diálogo Especificar contraseña. Escriba una contraseña de hasta 20 caracteres en el cuadro de texto que se proporciona y, a continuación, vuelva a escribir la misma contraseña en el cuadro de texto que aparece más abajo. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

  Siempre que se intente configurar las propiedades de una tarea protegida, la Consola pedirá al usuario la contraseña especificada. Al elegir esta opción, el usuario obtiene los mismos resultados que al activar la casilla de verificación **Tarea protegida por contraseña** en el cuadro de diálogo Propiedades de tarea.

- **Iniciar la Consola de VirusScan automáticamente.** Seleccione **Cargar al inicio** en el menú **Ver** para que la Consola de VirusScan se inicie cada vez que el usuario encienda el equipo. La Consola tiene activada esta opción de forma predeterminada. Como debe estar ejecutándose para que se lleven a cabo las tareas programadas, deberá optar por el inicio automático de la Consola de modo que las tareas programadas comiencen a la hora establecida.

  También puede controlar esta opción desde el panel de control de VirusScan.

- **Mostrar el icono de la bandeja del sistema de la Consola**. Seleccione **Mostrar icono de bandeja del sistema** en el menú **Ver** para que la Consola muestre este icono  en la bandeja del sistema de Windows. Haga doble clic en ese icono para que la ventana de la Consola aparezca en primer plano. Al hacer clic con el botón derecho del ratón en el icono aparece un menú de acceso directo.

- **Salir de la Consola de VirusScan.** Seleccione **Salir** en el menú **Tarea** para salir de la Consola. Si tiene pendiente alguna tarea, deberá minimizar la Consola en lugar de salir de la misma.

Trabajar con tareas predeterminadas

Tan pronto como instale en su equipo el software de VirusScan y lo reinicie, el software de VShield comenzará inmediatamente a explorar el sistema utilizando una configuración predeterminada, lo que ofrece una protección básica para el sistema. Las restantes tareas que aparecen en la ventana de la Consola también tienen definida su configuración, aunque permanecerán inactivas hasta que las active.

La Consola tiene cinco tareas predeterminadas. Son las siguientes:

- **VShield**. Esta tarea ejecuta el explorador VShield. De manera predeterminada, esta tarea se ejecuta automáticamente al iniciar el equipo. No puede programar el explorador VShield para que se ejecute en cualquier otro momento, pero es posible seleccionar diferentes opciones de exploración. No puede cambiar el nombre ni eliminar esta tarea, pero puede consultar las estadísticas referentes a la sesión de exploración más reciente, activarla o desactivarla y puede abrir el cuadro de diálogo Propiedades de VShield para configurarla.

- **Explorar Mi PC**. Esta tarea ejecuta una operación de exploración de base en todos los discos duros y otras unidades conectadas al equipo, junto con los sectores de arranque de la RAM, el disco duro y los disquetes. No puede cambiar el nombre ni eliminar esta tarea, pero puede modificar su configuración, programarla, consultar las estadísticas referentes a la operación de exploración más reciente y proteger su configuración con una contraseña. Deberá activar esta tarea para que se ejecute, pero puede ejecutarla en su configuración predeterminada para obtener una protección casi absoluta.

- **Explorar unidad 'C'**. Esta tarea ejecuta una operación de exploración de base en la unidad C: . Por lo demás, se parece mucho a la tarea Explorar Mi PC.

Tanto la tarea Explorar Mi PC como la tarea Explorar unidad 'C' necesitan la aplicación VirusScan para ejecutarse.

Trabajar con la tarea VShield

La tarea VShield aparece en la ventana de la Consola desde el principio de manera que es posible realizar la operación. Puede activarla y desactivarla directamente desde la ventana de la Consola o hacer doble clic en la tarea para abrir el cuadro de diálogo Propiedades de tarea (Figura 6-3).

Figura 6-3. Cuadro de diálogo Propiedades de tarea del explorador VShield

En este cuadro de diálogo, puede:

- **Activar o desactivar la tarea**. Haga clic en el botón **Desactivar** que se encuentra en la parte inferior del cuadro de diálogo Propiedades de tarea. Si el explorador se encuentra desactivado, este botón indicará **Activar**.
- **Abrir las páginas de propiedades de VShield**. Haga clic en **Configurar** para abrir el cuadro de diálogo Exploración de sistema, donde puede seleccionar todas las opciones de configuración que se encuentran disponibles en el explorador VShield.
- **Ver las estadísticas de los módulos de VShield**. Cada una de las demás páginas de propiedades en el cuadro de diálogo Propiedades de tarea muestra un resumen de las estadísticas correspondientes a la última sesión de exploración que realizó cada módulo. Haga clic en cualquier otra ficha para ver estas estadísticas.

Creación de nuevas tareas

Aunque las tareas que se incluyen en el conjunto predeterminado proporcionan una protección antivirus casi absoluta al sistema, probablemente desee crear y ejecutar tareas propias una vez que haya adquirido experiencia con el software de VirusScan y se haya hecho una idea de qué desea explorar y cuándo desea hacerlo.

Puede modificar algunos aspectos de las tareas predeterminadas que se encuentran en la Consola de VirusScan, pero no podrá eliminar, renombrar o (con la excepción de las tareas Explorar Mi PC y Explorar unidad 'C') crear nuevos ejemplos de ellas. Puede copiar las opciones de configuración existentes a partir de las tareas Explorar Mi PC y Explorar unidad 'C' para utilizar como opciones de base de nuevas tareas.

Sin embargo, la Consola permite crear hasta 50 nuevas tareas de acuerdo con sus necesidades. Podrá sobrepasar este límite cambiando el número en el panel de control de VirusScan.

Para crear una tarea nueva, realice los pasos siguientes:

1. Seleccione **Nueva tarea** en el menú **Tarea** en la ventana de la Consola, o haga clic en  en la barra de herramientas de la Consola.

Aparecerá el cuadro de diálogo Propiedades de tarea (Figura 6-4).

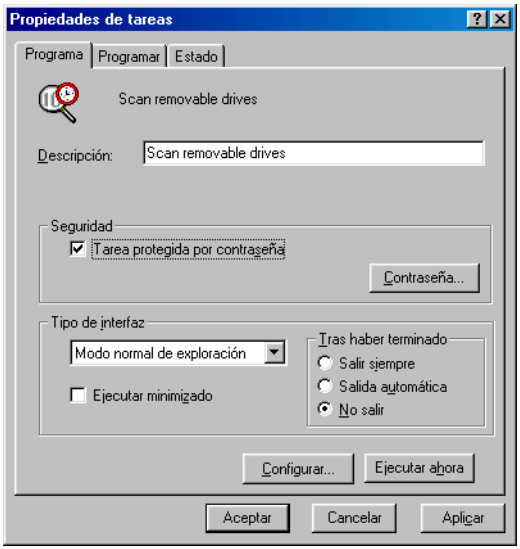

Figura 6-4. Cuadro de diálogo Propiedades de tarea: página Programa

2. Escriba un nombre para la tarea en el cuadro de texto Descripción.

   Asegúrese de que el nombre elegido describe la tarea de forma que pueda distinguirla de las demás tareas que figuran en la ventana de la Consola y pueda saber inmediatamente las operaciones que realiza.

3. Elija una contraseña para proteger esta tarea y evitar que algún usuario realice cambios en la configuración de la tarea de exploración. Para ello, siga estos pasos:

   a. Active la casilla de verificación **Tarea protegida por contraseña** y, a continuación, haga clic en **Contraseña** para abrir el cuadro de diálogo Especificar contraseña.

   b. Escriba una única contraseña en el cuadro de texto que se proporciona.

      Puede escribir un máximo de 20 caracteres de cualquier tipo. Asegúrese de seleccionar una contraseña que vaya a recordar.

   c. Vuelva a escribir una contraseña exactamente igual a la del cuadro de texto anterior.

   d. Active la casilla de verificación **Proteger todas las opciones** para proteger todas las opciones establecidas para esta tarea.

De esta manera, se bloquean inmediatamente todas las páginas de propiedades para esta tarea en la página Seguridad en el cuadro de diálogo Propiedades de VirusScan. Desactivar esta casilla de verificación permite seleccionar diferentes configuraciones de seguridad para cada página de la página de propiedades Seguridad.

e. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Especificar contraseña.

La Consola pedirá la contraseña siempre que algún usuario intente abrir el cuadro de diálogo Propiedades de tarea de esta tarea.

4. Especifique cómo debe aparecer la interfaz de tarea y el grado de control que desee tener sobre la tarea al ejecutarla. Podrá elegir entre las siguientes opciones:

- **Modo normal de exploración**. Esto muestra la ventana principal de la aplicación VirusScan durante las operaciones de exploración. Permite que cualquier usuario en cuyo equipo se ejecute la tarea vea, pero no cambie, las opciones de configuración que utiliza dicha tarea durante su ejecución, vea los resultados de la operación de exploración o detenga dicha operación en cualquier momento. También es posible seleccionar cualquier comando de los menús de la ventana principal.

  Active la casilla de verificación **Ejecutar minimizado** para iniciar la ventana como un botón minimizado en la barra de tareas de Windows.

- **Modo de sólo exploración**. Muestra una ventana mínima que indica que la tarea se está ejecutando. Puede detener, hacer una pausa o reanudar la tarea en cualquier punto.

  Active la casilla de verificación **Ejecutar minimizado** para iniciar la ventana como un botón minimizado en la barra de tareas de Windows.

- **Modo oculto**. No muestra ninguna interfaz mientras la tarea de exploración se está ejecutando. No puede realizar una pausa o detener la tarea a menos que la Consola de VirusScan o el cuadro de diálogo Propiedades de tarea se encuentren activados. La aplicación VirusScan le seguirá informando cuando encuentre un virus, si ha configurado alguna opción de alerta local para la tarea. Esta tarea siempre sale de la aplicación cuando termina.

5. Especifique lo que debe hacer la tarea cuando termine. Podrá elegir entre las siguientes opciones:

   - **Salir siempre**. Haga clic en este botón para indicarle a la aplicación VirusScan que siempre cierre inmediatamente después de realizar esta tarea de exploración. Si selecciona **Modo oculto** en la lista de tipo de interfaz, ésa será su opción única.

   - **Salida automática**. Haga clic en este botón para indicarle a la aplicación VirusScan que cierre automáticamente si no ha detectado ningún virus durante esta tarea de exploración. Si la aplicación encuentra un virus, permanecerá abierta para mostrar los resultados de la exploración.

     Si ejecuta la tarea en modo normal de exploración, le permitirá también eliminar los virus que detecte, siempre y cuando no haya configurado la aplicación para que lo haga automáticamente.

   - **No salir nunca**. Haga clic en este botón para indicarle a la aplicación VirusScan que siempre permanezca abierta después de realizar esta tarea de exploración.

     Si ejecuta la tarea en modo normal de exploración, se mostrarán los resultados de la operación de exploración y podrá eliminar los virus detectados siempre y cuando no la haya configurado para que lo haga automáticamente. A continuación, podrá volver a ejecutar inmediatamente la tarea si así lo desea.

6. En este momento, ya ha introducido suficiente información para crear la tarea, aunque aún no ha elegido ninguna opción de programa ni ha programado su ejecución. Podrá:

   - Hacer clic en **Configurar** para establecer las propiedades de esta tarea.

     Esto abre el cuadro de diálogo Propiedades de VirusScan. En este cuadro de diálogo podrá indicar a la aplicación VirusScan dónde y qué debe buscar durante la operación de exploración, cómo debe responder a los virus que encuentre, cómo debe notificarle cuando encuentre algún virus, qué información debe registrar en el correspondiente registro de actividades, qué elementos debe excluir de las tareas de exploración y si se deben proteger las opciones de configuración establecidas para la tarea.

   - Haga clic en **Ejecutar ahora** para ejecutar esta tarea inmediatamente. La tarea se ejecutará con las opciones de configuración predeterminadas o con las opciones de configuración que haya definido. Al hacer clic en el botón, ocurrirá lo siguiente:

  - Si ha configurado la tarea para que se inicie automáticamente, se ejecutará de forma inmediata. Para que sea así, es necesario haber activado previamente la casilla de verificación **Iniciar automáticamente** en el cuadro de diálogo Propiedades de VirusScan. Para ver esta casilla de verificación, haga clic en **Configurar**, que se encuentra justo a la izquierda y, a continuación, localice la casilla de verificación en el área Elementos a explorar de la página de propiedades Detección.
  - Si elige una tarea de exploración no configurada para que se inicie automáticamente, aparecerá la ventana de la aplicación VirusScan. Haga clic en **Explorar ahora** en esta ventana para que se ejecute la tarea.

- Haga clic en **Aplicar** para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de tarea y, a continuación, haga clic en la ficha Programar.
- Haga clic en **Aceptar** para guardar los cambios efectuados y volver a la ventana de la Consola de VirusScan. Posteriormente deberá configurar la programación de tareas para que se ejecute.

  Para ello, seleccione la tarea en la lista de la ventana de la Consola y, a continuación, haga clic en  para abrir el cuadro de diálogo Propiedades de tarea.
- Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin crear ninguna tarea.

Activar tareas

La activación de una tarea consiste en elegir una programación para la misma y activarla de forma que la tarea se ejecute cuando sea necesario. Es posible programar cualquiera de las tareas que aparecen en la ventana de la Consola de VirusScan, a excepción de la tarea VShield, que se ejecuta continuamente desde que inicia el equipo o tan pronto como inicia personalmente la tarea.

Para que se ejecute la tarea, también debe asegurarse de que la Consola de VirusScan esté activada en el momento que desea que se ejecute dicha tarea.

Para ejecutar una tarea de exploración que utiliza la aplicación VirusScan, es necesario configurar la operación de exploración para iniciarse automáticamente. No es necesario hacer esto para otras tareas predeterminadas. Consulte Paso 5 en la página 226 para obtener información detallada.

Para activar una tarea, realice los pasos siguientes:

1. Si todavía no tiene abierto el cuadro de diálogo Propiedades de tarea, haga doble clic en una de las tareas que aparecen en la lista de la ventana de la Consola, o seleccione una tarea y, a continuación, haga clic en  en la barra de herramientas de la Consola.

   Al hacerlo, aparecerá el cuadro de diálogo Propiedades de tarea (consulte la Figura 6-4 en la página 212).

2. Haga clic en la ficha Programar para que aparezca la página de propiedades adecuada (consulte la Figura 6-5).

   - **NOTA:** El cuadro de diálogo Propiedades de tarea del explorador VShield no incluirá una página de propiedades Programar sino páginas de estado para cada módulo del explorador.

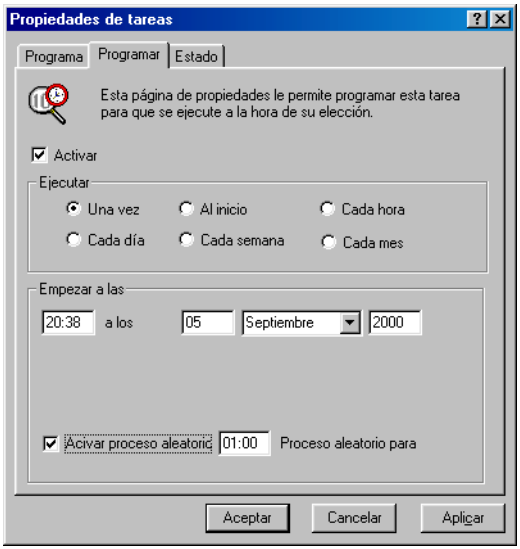

Figura 6-5. Cuadro de diálogo Propiedades de tarea - página Programar

3. Active la casilla de verificación **Activar**. Se activarán las opciones en las áreas Ejecución y Empezar a las.

4. Elija con qué frecuencia desea que se ejecute la tarea en el área Ejecución. Dependiendo del intervalo de tiempo seleccionado, el área Empezar a las ofrecerá diferentes opciones para la programación de la tarea. Las opciones son las siguientes:

- **Una vez**. Esta opción ejecuta su tarea una sola vez en la fecha y hora que especifique. Introduzca la hora en el cuadro de texto situado más a la izquierda en el área Empezar a las y, a continuación, seleccione un mes en la lista de la derecha. Después, introduzca el día y el año en los cuadros de texto correspondientes.
- **Diaria**. Esta opción ejecuta la tarea una vez a la hora que especifique y en los días que indique. Escriba la hora en el cuadro de texto correspondiente y, a continuación, active las casillas de verificación del área Empezar a las correspondientes a los días que desee ejecutar la tarea.
- **Al iniciar**. Active esta casilla de verificación para ejecutar la tarea cada vez que inicie el equipo y la Consola de VirusScan. Especifique en horas y minutos el tiempo después de iniciar el sistema que desea que la Consola espere antes de ejecutar la tarea. *No* se puede establecer esta programación de forma aleatoria.
- **Semanal**. Esta opción ejecuta la tarea una vez a la semana en el día y a la hora que especifique. Escriba la hora en el cuadro de texto correspondiente y, a continuación, seleccione un día en la lista de la derecha.
- **Cada hora**. Esta opción ejecuta la tarea cada hora siempre que el equipo esté encendido y la Consola esté funcionando. Especifique en el cuadro de texto correspondiente los minutos que debe esperar la Consola después de cada ahora para ejecutar la tarea.
- **Mensual**. Esta opción ejecuta la tarea una vez al mes en el día y a la hora que especifique. Escriba la hora en el cuadro de texto situado más a la izquierda y, a continuación, el día del mes en el que desea ejecutar la tarea.

- **NOTA:** Escriba todas las horas de programación utilizando el formato de 24 horas, excepto en el caso de intervalos de tiempo cada hora. Si desea que una tarea se ejecute a las 9:30 p.m., por ejemplo, deberá escribir 21:30.

---

5. Para ejecutar esta tarea en un intervalo de tiempo aleatorio dentro del tiempo establecido, active la casilla de verificación **Activar proceso aleatorio** y, a continuación, introduzca un período de tiempo de hasta ocho horas en el cuadro de texto Proceso aleatorio para ventana de tiempo.

   A menos que haya configurado esta tarea para que se ejecute al iniciar, con esta función se reducirá el tráfico en la red y cualquier otro tipo de sobrecarga en el sistema que pueda surgir del hecho de existir simultáneamente varias operaciones de actualización y de ejecución del equipo. La tarea se ejecutará en un punto aleatorio dentro de la "ventana" de tiempo que se especifique.

La ventana se centra en el tiempo programado para la ejecución de la tarea. Si, por ejemplo, establece esta tarea para que se ejecute todos los días a las 15:00, ha seleccionado **Activar proceso aleatorio** y especificado una ventana de tiempo de una hora, la tarea se ejecutaría en cualquier momento entre las 14:30 y las 15:30. Es posible establecer una ventana de hasta 480 minutos u ocho horas.

6. Ahora ya tiene definida una programación para la tarea y está listo para que se ejecute en el momento previsto. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Propiedades de tarea, o haga clic en **Aplicar** para guardar las opciones seleccionadas sin cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Para iniciar la tarea, el equipo deberá estar encendido y la Consola de VirusScan deberá estar funcionando. Si su equipo está apagado o si la Consola no se ejecuta a la hora a la que tiene que iniciarse la tarea, ésta se iniciará a la siguiente hora que tenga programada. Puede minimizar la Consola para que aparezca únicamente como un icono en la barra de tareas de Windows.

  Si desea que la aplicación VirusScan ejecute una tarea de exploración en un equipo sin supervisión, debe configurar también el programa para que inicie automáticamente su operación de exploración. Consulte el Paso 5 en la página 226 si desea obtener más información.

Comprobación del estado de la tarea

La ventana de la Consola de VirusScan recoge la fecha y la hora a la que las tareas se ejecutaron por última vez y están programadas para ejecutarse de nuevo; esta información aparece a la derecha de cada una de las tareas que figuran en la lista. También puede ver un resumen de los archivos explorados por cada tarea, los agentes perjudiciales eventualmente detectados y las medidas que se han tomado.

Para ver los resultados de las tareas, siga los siguientes pasos:

1. Si todavía no tiene abierto el cuadro de diálogo Propiedades de tarea, haga doble clic en una de las tareas que aparecen en la lista de la ventana de la Consola, o seleccione una tarea y, a continuación, haga clic en  en la barra de herramientas de la Consola.
2. Al hacerlo, aparecerá el cuadro de diálogo Propiedades de tarea (consulte la Figura 6-4 en la página 212). Haga clic en la ficha Estado para que aparezca la página de propiedades adecuada (Figura 6-6 en la página 219).

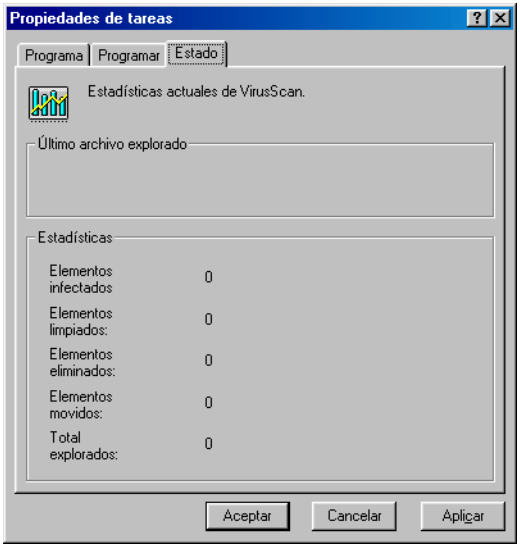

Figura 6-6. Cuadro de diálogo Propiedades de tarea: página Estado

La página de estado mostrará una lista con los resultados de la última exploración que llevó a cabo esta tarea, así como el nombre del último archivo explorado. Para ver una breve descripción de cada uno de los elementos que aparecen en esta página, haga clic con el botón derecho del ratón en una figura o etiqueta y, a continuación, seleccione **¿Qué es esto?** en el menú de acceso directo que aparece o haga clic en el botón **?** que aparece en la esquina superior derecha del cuadro de diálogo y, por último, haga clic en el elemento cuya descripción desee ver. Estas pantallas *no* se actualizarán en tiempo real.

- **NOTA:** El cuadro de diálogo Propiedades de tarea de la tarea VShield incluirá las páginas de estado de todos los módulos de VShield.

Configuración de las opciones de la aplicación VirusScan

Para configurar una tarea de exploración de VirusScan que se ejecutará cuando el usuario estime oportuno, debe indicárselo a la aplicación:

- Cuando desea que se ejecute
- qué debe explorar
- qué desea que haga cuando detecte un virus
- cómo debe avisar cuando detecte un virus
- si debe llevar un registro de las acciones
- qué elementos no desea explorar en busca de virus
- si desea proteger las opciones elegidas frente a cambios no autorizados

La Consola de VirusScan proporciona una serie de páginas de propiedades que puede utilizar para definir la tarea. Esta página de propiedades reproduce muchas de las opciones que aparecen en la ventana principal de la aplicación VirusScan y agrega otras que pueden ayudarle a definir una tarea que desee ejecutar de forma habitual y repetida.

Para configurar la aplicación VirusScan con el fin de que ejecute una tarea de exploración, seleccione una de todas las que aparecen en la lista de la ventana de la Consola, incluida cualquier tarea que haya creado por su cuenta, y , a continuación, haga clic en  en la barra de herramientas de la Consola.

Aparecerá el cuadro de diálogo Propiedades de VirusScan (Figura 6-7).

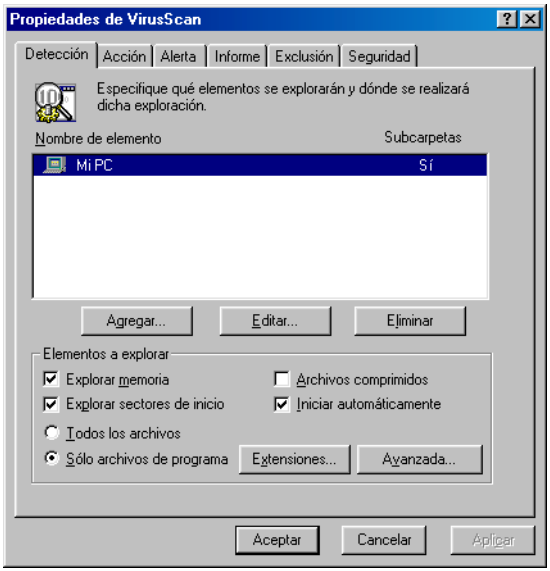

Figura 6-7. Cuadro de diálogo Propiedades de VirusScan: página Detección

Selección de las opciones de Detección

Si desea configurar una tarea que acaba de crear, la aplicación VirusScan inicialmente considera que desea explorar la unidad C: y la memoria del equipo, buscar virus en el sector de arranque y limitar los archivos que explora sólo a aquellos que tienen mayores probabilidades de ser infectados. Si decide configurar una de las tareas predeterminadas, las opciones iniciales variarán.

Para modificar las opciones de tarea iniciales, realice el siguiente procedimiento:

1. Elija las partes del sistema o de la red que desea que explore la aplicación VirusScan en busca de virus. Podrá:

   - **Agregar objetivos de exploración.** Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar elemento de exploración (Figura 6-8).

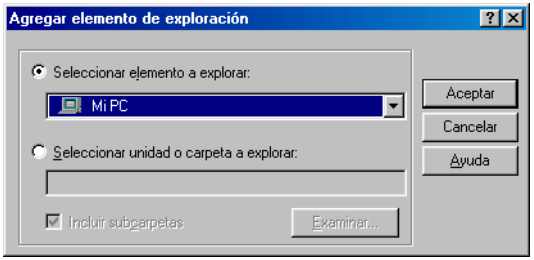

Figura 6-8. Cuadro de diálogo Agregar elemento de exploración

Para explorar todo el equipo o un subgrupo de las unidades del sistema o de la red, haga clic en el botón **Seleccionar elemento a explorar**, a continuación:

a. Seleccione un objetivo que desee explorar en la lista que se proporciona. Podrá elegir entre las siguientes opciones:

   – **Mi PC**. Indica a la aplicación que explore todas las unidades que estén conectadas físicamente al equipo o mediante la asignación de unidades a través del explorador de Windows a una letra de unidad del equipo.

   – **Todos los medios extraíbles**. Indica a la aplicación que explore sólo los disquetes, discos CD-ROM, discos ZIP Iomega o dispositivos de almacenamiento similares que estén conectados físicamente al equipo.

   – **Todos los discos duros**. Indica a la aplicación que explore los discos duros que estén conectados físicamente al equipo.

   – **Todas las unidades de red**. Indica a la aplicación que explore todas las unidades asignadas mediante el explorador de Windows a una letra de unidad del equipo.

b. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Para explorar un disco o una carpeta en concreto del sistema, haga clic en el botón **Seleccionar unidad o carpeta a explorar**, a continuación:

a. Escriba en el cuadro de texto correspondiente la letra de unidad o la ruta de acceso a la carpeta que desea explorar, o haga clic en **Examinar** para buscar el objetivo de exploración en el equipo.

- **NOTA:** No se puede utilizar la notación de la Convención de nomenclatura universal (UNC) para especificar un disco de red como objetivo de exploración de tareas programadas. Si lo hace, obtendrá como resultado un error de ruta no válida. Puede utilizar la notación UNC para especificar objetivos de exploración para operaciones que ejecute directamente con la aplicación VirusScan.

b. Active la casilla de verificación**Incluir subcarpetas** para que la aplicación VirusScan busque virus en las carpetas que pueda haber en el objetivo de exploración.

- **NOTA:** Al elegir **Incluir subcarpetas** la aplicación realiza una exploración sólo en aquellos archivos almacenados en las propias subcarpetas. La aplicación no explorará los archivos almacenados en el directorio raíz de la carpeta designada. Para explorar esos archivos, desactive la casilla de verificación **Incluir subcarpetas**.

c. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Cambiar los objetivos de exploración.** Seleccione uno de los objetivos de exploración de la lista y haga clic en **Editar** para abrir el cuadro de diálogo Editar elemento de exploración (Figura 6-9).

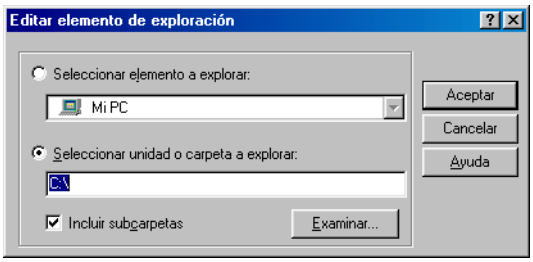

Figura 6-9. Cuadro de diálogo Editar elemento de exploración

En el cuadro de diálogo aparecerá seleccionado el objetivo de exploración existente. Seleccione o escriba un nuevo objetivo de exploración y, a continuación, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Eliminar objetivos de exploración.** Seleccione uno de los objetivos de exploración detallados y haga clic en **Eliminar** para eliminarlo.

2. Especifique los tipos de archivos que desea que examine la aplicación VirusScan. Podrá:

- **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que la aplicación VirusScan busque virus en archivos comprimidos y archivos de almacenamiento. Aunque esta opción proporciona mayor protección, la exploración de archivos comprimidos puede aumentar la cantidad de tiempo necesario para las operaciones de exploración.
- **Explorar todos los archivos**. Active la casilla de verificación **Todos los archivos** para que la aplicación explore todos los archivos del destino especificado sea cual sea la extensión.

- **NOTA:** McAfee VirusScan Software recomienda que seleccione esta opción la primera vez que realice una exploración y periódicamente en futuras ocasiones, para asegurarse de que el sistema no contiene virus. De este modo, puede limitar el ámbito de operaciones de exploración posteriores.

- **Seleccionar los tipos de archivos**. Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea archivos de comandos, macros o códigos binarios. Por tanto, podrá reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, limitándolo a los archivos con mayores probabilidades de ser infectados. Para ello, haga clic en el botón **Sólo archivos de programa**.

  Para ver o designar las extensiones de nombres de archivo que la aplicación examinará, haga clic en **Extensiones**. De este modo se abre el cuadro de diálogo Extensiones de archivos de programa.

3. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración (Figura 6-10).

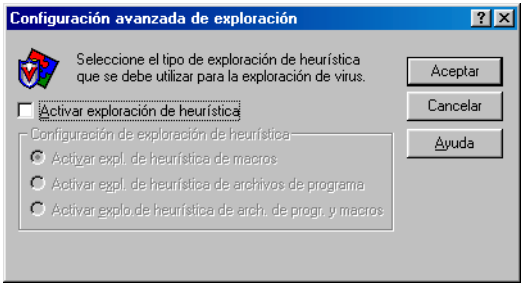

Figura 6-10. Cuadro de diálogo Configuración avanzada de exploración

La tecnología de exploración heurística permite a la aplicación VirusScan reconocer nuevos virus basándose en su parecido a virus similares que el módulo ya conoce. Para hacerlo, la aplicación busca determinadas características "tipo virus" en los archivos especificados para explorar. La presencia de una cantidad suficiente de estas características en un archivo lleva a la aplicación a identificarlo como posiblemente infectado con un nuevo virus o con uno que aún no ha sido identificado.

Puesto que la aplicación busca simultáneamente características en el archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas de infección. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

La aplicación VirusScan se inicia sin ninguna opción de exploración heurística activa. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que desee que la aplicación VirusScan utilice. Podrá elegir entre las siguientes opciones:

   - **Activar expl. de heurística de macros**. Elija esta opción para que la aplicación identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que incluyan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. La aplicación identificará las coincidencias totales con el nombre del virus correspondiente. Cuando las firmas del código recuerden a virus existentes, dicha aplicación indicará que ha encontrado un posible virus de macro.

   - **Activar expl. de heurística de arch. de programa.** Elija esta opción para que la aplicación VirusScan localice nuevos virus en archivos de programa examinando sus características y comparándolas con una lista de características de virus conocidos. La aplicación identificará los archivos que tengan un número suficiente de estas características como posibles virus.

   - **Activar expl. de heurística de arch. de programa y macros.** Elija esta opción para que la aplicación utilice ambos tipos de exploración heurística. McAfee VirusScan Software aconseja el uso de esta opción para obtener una protección antivirus total.

- **NOTA:** La aplicación utilizará técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide examinar **Todos los archivos**, utilizará una exploración heurística para todos los tipos de archivos.

c. Haga clic en **Aceptar** para guardar los cambios y volver al cuadro de diálogo Propiedades de VirusScan.

4. Elija otras opciones de exploración.

   Los virus del sector de arranque se cargan en la memoria de los equipos y se ocultan en los bloques de arranque o en el registro de arranque principal del disco duro. Para utilizar esta tarea de exploración con el fin de detectar esos tipos de virus, active las casillas de verificación **Explorar memoria** y **Explorar sectores de inicio**.

5. Si ha programado operaciones de exploración que desea que se ejecuten en su ausencia, active la casilla de verificación **Iniciar automáticamente** para indicar a la aplicación VirusScan que debe comenzar la exploración en cuanto se inicie.

   Si no selecciona esta casilla, la Consola iniciará el software de VirusScan, pero la aplicación VirusScan esperará a que haga clic en **Explorar ahora** para comenzar la exploración. Si no selecciona dicha casilla de verificación, tiene la posibilidad de cancelar la operación de exploración si interfiere en su trabajo.

6. Haga clic en la ficha Acción para seleccionar otras opciones de VirusScan. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de VirusScan, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y volver a la ventana de la Consola. Haga clic en **Cancelar** para volver a la ventana de la Consola sin guardar los cambios.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Acción

Cuando la aplicación VirusScan detecta un virus, puede responder preguntando qué debe hacer con el archivo infectado o emprendiendo automáticamente la acción que se le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta desea que el software de VirusScan le ofrezca cuando encuentre un virus o qué acciones desea que emprenda automáticamente.

Siga estos pasos:

1. Para empezar desde la ventana de la Consola, seleccione la tarea creada en la lista de tareas y, a continuación, haga clic en  en la barra de herramientas de la Consola.

2. Aparecerá el cuadro de diálogo Propiedades de VirusScan (vea la Figura 6-7 en la página 221). Haga clic en la ficha Acción para que aparezca la página de propiedades adecuada (vea la Figura 6-11 en la página 227).

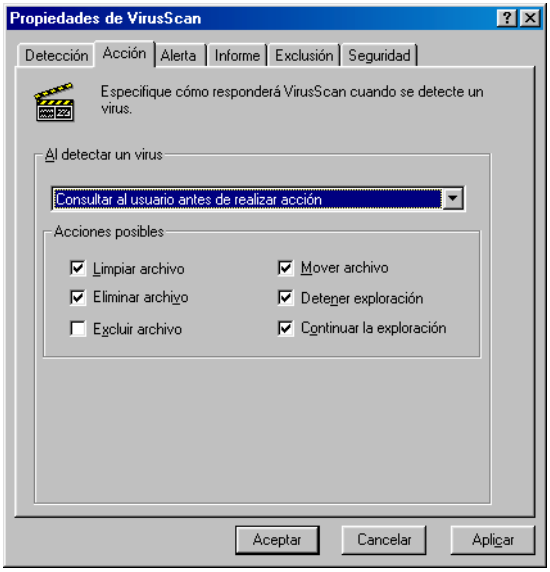

Figura 6-11. Cuadro de diálogo Propiedades de VirusScan: página Acción

3. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada inmediatamente debajo de la lista cambiará para mostrar opciones adicionales para cada respuesta. Podrá elegir entre las siguientes opciones:

   - **Consultar al usuario antes de realizar acción.** Elija esta respuesta si espera estar trabajando con el equipo cuando la aplicación VirusScan explore el disco. El programa presentará mensajes de alerta cuando encuentre un virus y le ofrecerá una gama de posibles respuestas.

     Cada casilla de verificación que se active en la página Acción hace que aparezca un botón en el mensaje de alerta que la aplicación muestra cuando encuentra un virus. Por ejemplo, al seleccionar **Eliminar archivo**, aparecerá el botón **Eliminar** en el mensaje de alerta.

Puede seleccionar una de las siguientes opciones:

- **Limpiar archivo**. Esta opción indica a la aplicación que intente eliminar el código de virus del archivo infectado. Si la función de elaboración de informes está activada, grabará un suceso de registro cada vez que limpie o no pueda limpiar un archivo infectado.
- **Eliminar archivo**. Esta opción indica a la aplicación que elimine inmediatamente el archivo infectado.
- **Excluir archivo.** Esta opción indica a la aplicación que ignore el archivo durante las operaciones de exploración posteriores. Es la única opción cuya selección no está predeterminada.
- **Continuar la exploración**. Esta opción indica a la aplicación que continúe con la exploración, pero que no emprenda ninguna otra acción. Si las opciones de generación de informes están activadas, la aplicación incluirá el incidente en su archivo de registro.
- **Detener exploración**. Esta opción indica a la aplicación que detenga inmediatamente la operación de exploración. Para continuar, debe hacer clic en **Explorar ahora** para reiniciar la operación.
- **Mover archivo**. Esta opción indica a la aplicación que desplace el archivo infectado a una carpeta de cuarentena. Los mensajes de alerta mostrarán un botón **Mover archivo a** que el usuario puede utilizar para buscar una carpeta de cuarentena.

- **Mover archivos infectados automáticamente**. Elija esta respuesta para que la aplicación mueva los archivos infectados a la carpeta de cuarentena.

  De forma predeterminada, la aplicación mueve estos archivos a una carpeta denominada \Infectados en el directorio de programa de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente o hacer clic en **Examinar** para encontrar una carpeta adecuada en su disco duro.

- **Limpiar los archivos infectados automáticamente**. Elija esta respuesta para indicar a la aplicación que elimine el código de virus del archivo infectado tan pronto como lo detecte. Si la aplicación no puede eliminar el virus, anotará el incidente en el archivo de registro.

- **Eliminar los archivos infectados automáticamente**. Elija esta opción si desea que la aplicación elimine inmediatamente todos los archivos infectados que detecte. Asegúrese de activar la función de generación de informe para poder tener un registro de todos los archivos que la aplicación haya eliminado. Tendrá que recuperar los archivos eliminados de las copias de seguridad. Si la aplicación no puede eliminar el archivo infectado, anotará el incidente en el archivo de registro.
- **Continuar la exploración**. Utilice esta opción sólo si prevé dejar el equipo sin atención mientras la aplicación comprueba si hay virus. Si también activa la función de generación de informes, la aplicación registrará los nombres de los virus que encuentre y de los archivos infectados para que los elimine tan pronto como tenga la oportunidad.

4. Haga clic en la ficha Alerta para seleccionar otras opciones de VirusScan. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de VirusScan, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y volver a la ventana de la Consola. Haga clic en **Cancelar** para volver a la ventana de la Consola sin guardar los cambios.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Alerta

Una vez configurada la aplicación VirusScan con las opciones de respuesta que desee, puede dejar que busque y elimine automáticamente virus del sistema, conforme los vaya encontrando, sin apenas intervención posterior. Para que la aplicación le informe automáticamente de que ha encontrado un virus con el fin de tomar las medidas apropiadas, es necesario configurarlo para que le envíe el correspondiente mensaje de alerta.

Siga estos pasos:

1. Para empezar desde la ventana de la Consola, seleccione la tarea creada en la lista de tareas y, a continuación, haga clic en  en la barra de herramientas de la Consola.
2. Aparecerá el cuadro de diálogo Propiedades de VirusScan (vea la Figura 6-7 en la página 221). Haga clic en la ficha Alerta para que aparezca la página de propiedades adecuada (Figura 6-12 en la página 230).

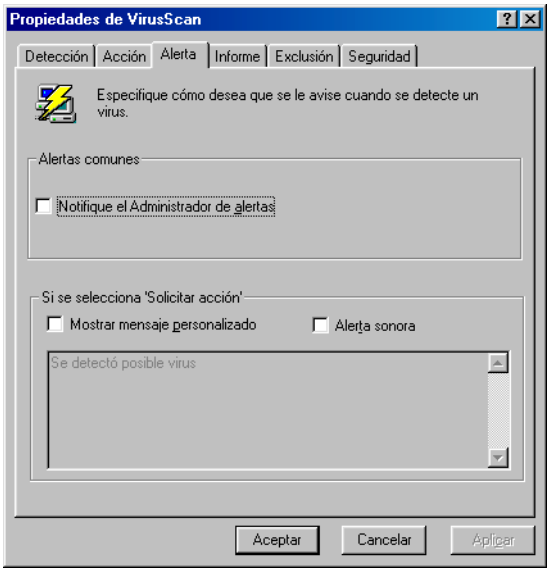

Figura 6-12. Cuadro de diálogo Propiedades de VirusScan: página Alerta

3. Active la casilla de verificación **Notificar al Administrador de alertas** para que la aplicación VirusScan envíe mensajes de alerta al Administrador de alertas para su distribución.

   El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que la aplicación VirusScan envíe satisfactoriamente estos mensajes de alerta, debe configurar la utilidad de configuración de cliente del Administrador de alertas.

   Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

   - **NOTA:** Si se desactiva esta casilla de verificación, la aplicación VirusScan no enviará ningún mensaje de alerta mediante el Administrador de alertas; sin embargo, esto no afecta a otros mensajes de alerta configurados en esta página de propiedades.

4. Active la casilla de verificación **Alerta sonora** para que la aplicación emita un sonido cuando encuentre un archivo infectado.

   Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**. La aplicación hará sonar un sonido estándar de alerta del sistema o hará que el equipo ejecute el archivo .WAV que se haya definido previamente.

5. Active la casilla de verificación **Mostrar mensaje personalizado** para que la aplicación agregue un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

   Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

6. Escriba el mensaje que desee que muestre la aplicación en el cuadro de texto proporcionado. Puede escribir 250 caracteres como máximo.

7. Haga clic en la ficha Informe para seleccionar otras opciones de VirusScan. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de VirusScan, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y volver a la ventana de la Consola. Haga clic en **Cancelar** para volver a la ventana de la Consola sin guardar los cambios.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Informe

La aplicación VirusScan enumera la configuración actual y resume todas las acciones que emprende durante las operaciones de exploración en un archivo de registro denominado VSCLOG.TXT. Puede hacer que la aplicación escriba su registro en ese archivo o puede utilizar cualquier editor de textos para crear un archivo de texto con el fin de que lo utilice la aplicación. Después podrá abrir e imprimir el archivo de registro para examinarlo posteriormente desde la aplicación o desde el editor de texto.

El archivo VSCLOG.TXT puede ser una herramienta muy importante para efectuar un seguimiento de la actividad de los virus en su sistema y tomar nota de los parámetros de configuración utilizados para detectar y responder a las infecciones que encuentre la aplicación VirusScan. También puede utilizar los informes de incidentes que se registran en el archivo para determinar qué archivos tiene que reemplazar a partir de las copias de seguridad, cuáles debe examinar de los que se encuentran en el área de cuarentena y cuáles debe eliminar del equipo. Utilice la página de propiedades Informes para determinar qué información debe incluir el software de VirusScan en su archivo de registro.

Para decidir qué datos registrará la aplicación y qué longitud podrá alcanzar el archivo de registro, siga los siguientes pasos:

1. Para empezar desde la ventana de la Consola, seleccione la tarea creada en la lista de tareas y, a continuación, haga clic en  en la barra de herramientas de la Consola.

2. Aparecerá el cuadro de diálogo Propiedades de VirusScan (vea la Figura 6-7 en la página 221). Haga clic en la ficha Informe para que aparezca la página de propiedades adecuada (Figura 6-13).

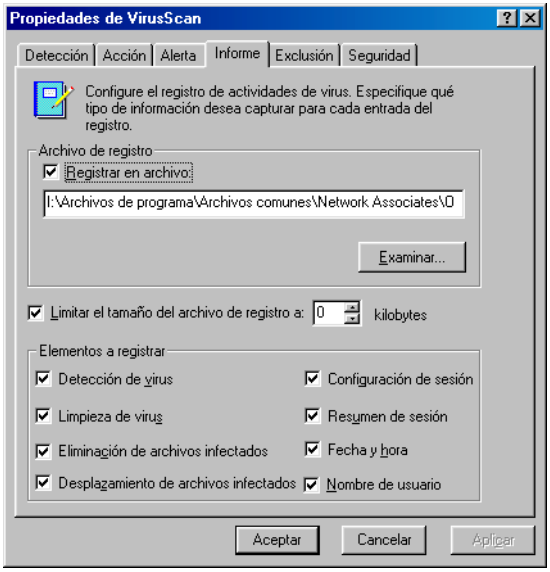

Figura 6-13. Propiedades de VirusScan: página Informe

3. Active la casilla de verificación **Registrar en archivo**.

   Como opción predeterminada, la aplicación VirusScan escribe la información de registro en el archivo VSCLOG.TXT, en el directorio de programa de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente, o hacer clic en **Examinar** para encontrar un archivo adecuado en su disco duro o en la red. Puede utilizar un archivo diferente, pero debe existir el archivo de texto. La aplicación no creará ningún archivo nuevo.

4. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente. Si no activa esta casilla de verificación, el tamaño del archivo de registro puede aumentar tanto como el espacio en disco lo permita.

   Escriba un valor entre 10 KB y 999 KB. Como opción predeterminada, la aplicación limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, la aplicación eliminará el registro existente y comenzará de nuevo desde el punto en el que se quedó.

5. Active las casillas de verificación que correspondan a la información que desea que la aplicación incluya en el archivo de registro. Cada casilla de verificación que se selecciona aquí hace que la aplicación registre esa información, normalmente cuando la exploración finaliza, o cuando el usuario apaga el sistema:

   - **Detección de virus**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación encuentre durante cada operación de exploración. Desactive la casilla de verificación para no incluir esta información en el archivo de registro.
   - **Limpieza de virus**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación limpie o intente limpiar durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
   - **Eliminación de archivos infectados**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación elimine durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

- **Desplazamiento de archivos infectados**. Active esta casilla de verificación para que el archivo de registro recoja la cantidad de virus que la aplicación mueva a una carpeta de cuarentena durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Configuración de sesión**. Active esta casilla de verificación para que el archivo de registro recoja las opciones de configuración utilizadas por la aplicación durante cada operación de configuración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Resumen de sesión**. Active esta casilla de verificación para que el archivo de registro haga un resumen de las acciones que la aplicación realizó durante cada operación de exploración.
  El registro incluirá:
  - Número de archivos que la aplicación ha examinado.
  - Número de archivos infectados que la aplicación ha limpiado.
  - Número de archivos infectados que la aplicación ha eliminado.
  - Número de archivos infectados que la aplicación ha movido a una carpeta de cuarentena.
  - Las opciones de configuración de la aplicación.

  Desactive la casilla de verificación para no incluir esta información en el archivo de registro.
- **Fecha y hora**. Active esta casilla de verificación para que se escriban en el archivo de registro la fecha y la hora a la que el software comenzó la operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Nombre de usuario**. Active esta casilla de verificación para que el archivo de registro recoja el nombre de usuario registrado en la estación de trabajo cuando el software inicie cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

Para ver el contenido del archivo de registro desde la Consola de VirusScan, seleccione la tarea que creó en la lista de tareas y, a continuación, elija **Ver registro de actividades** en el menú **Tarea**. También puede iniciar la aplicación VirusScan y seleccionar **Ver registro de actividades** en el menú **Archivo**.

6. Haga clic en la ficha Exclusión para seleccionar otras opciones de VirusScan. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de VirusScan, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y volver a la ventana de la Consola. Haga clic en **Cancelar** para volver a la ventana de la Consola sin guardar los cambios.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Exclusión

Muchos de los archivos que contiene el equipo no pueden infectarse. Las operaciones de exploración que examinan esos archivos pueden tardar mucho tiempo y producen escasos resultados. Puede acelerar las operaciones de exploración indicando a la aplicación VirusScan que sólo examine los tipos de archivos que tienen probabilidades de estar infectados o indicarle que excluya archivos y carpetas completas que sabe que no se infectarán.

Una vez que haya explorado exhaustivamente el sistema, puede excluir los archivos y carpetas que no cambian o aquellos que no suelen ser vulnerables a infecciones de virus. Además puede confiar en el explorador VShield para disponer de protección entre las operaciones de exploración programadas. Sin embargo, la realización de operaciones periódicas de exploración que examinen todas las zonas del equipo constituye la mejor defensa contra los virus.

Para evitar que la exploración examine los archivos no se infectan, puede identificar los discos, carpetas o archivos individuales que desea excluir de las operaciones de exploración en una lista de exclusión. De forma predeterminada, la aplicación VirusScan no explora la Papelera de reciclaje, ya que Windows no ejecutará los elementos que se hayan almacenado en dicho lugar. Por lo tanto, dichos elementos aparecerán en la lista de exclusión la primera vez que se abra la ventana.

Cada registro de la lista de exclusión muestra la ruta del elemento, especifica si la aplicación también excluirá cualquier carpeta anidada del objetivo y explica si la aplicación excluirá el elemento al explorar los archivos, cuando explore el sector de arranque del disco duro o en ambos casos.

Puede excluir de forma predeterminada hasta 100 objetivos únicos de exploración. Para cambiar este número, abra el panel de control de VirusScan, haga clic en la ficha Componentes y, a continuación, inserte una nueva cifra en el cuadro de texto **Número máximo de elementos excluidos**.

Para excluir archivos o carpetas de las actividades de exploración, siga estos pasos:

1. Para empezar desde la ventana de la Consola, seleccione la tarea creada en la lista de tareas y, a continuación, haga clic en  en la barra de herramientas de la Consola.

2. Aparecerá el cuadro de diálogo Propiedades de VirusScan (vea la Figura 6-7 en la página 221). Haga clic en la ficha Exclusión para que aparezca la página de propiedades adecuada. (Figura 6-14).

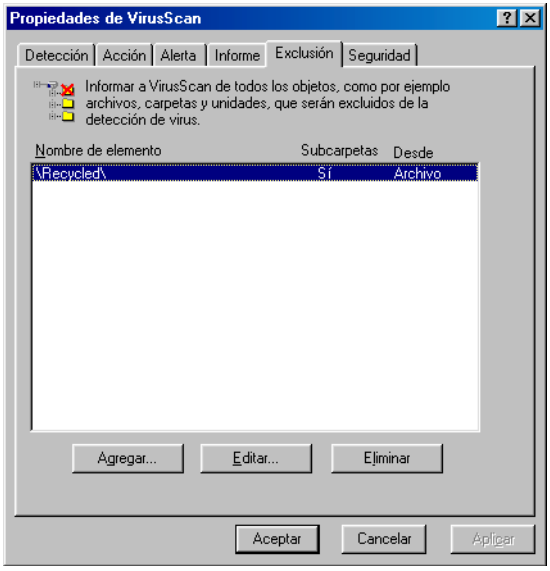

Figura 6-14. Cuadro de diálogo Propiedades de VirusScan: página Exclusión

3. Especifique los elementos que desea excluir. Podrá:

   - **Agregar archivos, carpetas o volúmenes a la lista de exclusión.** Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar elemento de exclusión (Figura 6-15).

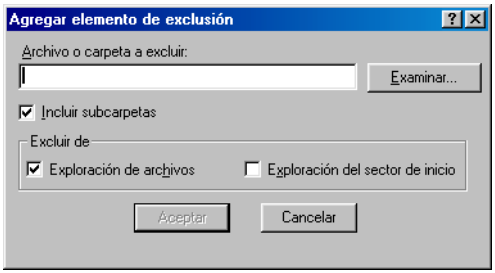

Figura 6-15. Cuadro de diálogo Agregar elemento de exclusión

A continuación, siga los siguientes pasos para agregar elementos a la lista:

a. Escriba una ruta en una carpeta o un nombre de archivo en el cuadro de texto que se proporciona o haga clic en **Examinar** para buscar el elemento que desea que la aplicación excluya.

- **NOTA:** Si ha elegido mover los archivos infectados automáticamente a una carpeta de cuarentena, la aplicación excluirá esa carpeta de las operaciones de exploración.

---

b. Active la casilla de verificación **Incluir subcarpetas** para indicar a la aplicación que ignore los archivos almacenados en cualquier subcarpeta de la carpeta especificada en el Paso a.

- **NOTA:** Al elegir **Incluir subcarpetas** la aplicación ignorará sólo aquellos archivos almacenados en las propias subcarpetas. La aplicación todavía explorará los archivos almacenados en el directorio raíz de la carpeta que indique. Para excluir los archivos del directorio raíz, desactive la casilla de verificación **Incluir subcarpetas**.

---

c. Active la casilla de verificación **Exploración de archivos** para excluir el elemento especificado en el primer paso de las operaciones de exploración en las que la aplicación busca virus que infecten archivos. Normalmente, estos virus aparecen en archivos que forman parte de las partes visibles del disco duro.

d. Active la casilla de verificación **Exploración del sector de inicio** para excluir el elemento especificado en el primer paso de las operaciones de exploración en las que la aplicación busca virus en el sector de arranque.

Estos virus normalmente aparecen en la memoria o en los archivos que residen en el sector de arranque o el registro de arranque principal del disco duro. Utilice esta opción para excluir archivos del sistema, como COMMAND.COM, de las operaciones de exploración.

+ **ADVERTENCIA:** McAfee VirusScan aconseja *no* excluir los archivos de sistema de las operaciones de exploración.

---

e. Repita del Paso a. al Paso d. hasta que haya incluido en la lista todos los archivos y carpetas que no desee explorar.

- **Modificar la lista de exclusión.** Para cambiar la configuración de un elemento de exclusión, selecciónelo en la lista de exclusiones y, seguidamente, haga clic en **Editar** para abrir el cuadro de diálogo Editar elemento de exclusión. Efectúe los cambios necesarios y haga clic en **Aceptar** para cerrar el cuadro de diálogo.
- **Eliminar un elemento de la lista.** Para eliminar un elemento de exclusión, selecciónelo en la lista y haga clic en **Eliminar**. Esto significa que la aplicación VirusScan *explorará* este archivo o carpeta durante la siguiente operación de exploración.

4. Haga clic en la ficha Seguridad para seleccionar otras opciones de VirusScan. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de VirusScan, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y volver a la ventana de la Consola. Haga clic en **Cancelar** para volver a la ventana de la Consola sin guardar los cambios.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Seguridad

El software de VirusScan le permite establecer una contraseña para proteger los valores de configuración seleccionados en cada página de propiedades frente a cambios no autorizados. Esta función es muy útil para administradores de sistema que deseen impedir que los usuarios manipulen sus medidas de seguridad mediante el cambio de las opciones de configuración de VirusScan. Utilice la página Seguridad para bloquear las configuraciones realizadas.

También puede proteger todas las opciones de esta tarea de una sola vez sin seleccionar páginas individuales. Para ello, seleccione la tarea de la ventana de la Consola y, a continuación, elija **Tarea de protección de contraseña** en el menú **Tarea**.

También puede hacer doble clic en cualquier tarea para abrir el cuadro de diálogo Propiedades de tarea. Desde este cuadro de diálogo puede activar la casilla de verificación **Tarea protegida por contraseña** y, a continuación, hacer clic en **Contraseña** para asignar una contraseña. Escriba la contraseña que desee utilizar, seguidamente active la **casilla de verificación Proteger todas las opciones** para proteger todas las páginas de propiedades de la aplicación VirusScan de una sola vez.

Para proteger opciones de tareas individuales, siga los siguientes pasos:

1. Para empezar desde la ventana de la Consola, seleccione la tarea creada en la lista de tareas y, a continuación, haga clic en  en la barra de herramientas de la Consola.

2. Aparecerá el cuadro de diálogo Propiedades de VirusScan (vea la Figura 6-7 en la página 221). Haga clic en la ficha Seguridad para que aparezca la página de propiedades adecuada (vea la Figura 6-16).

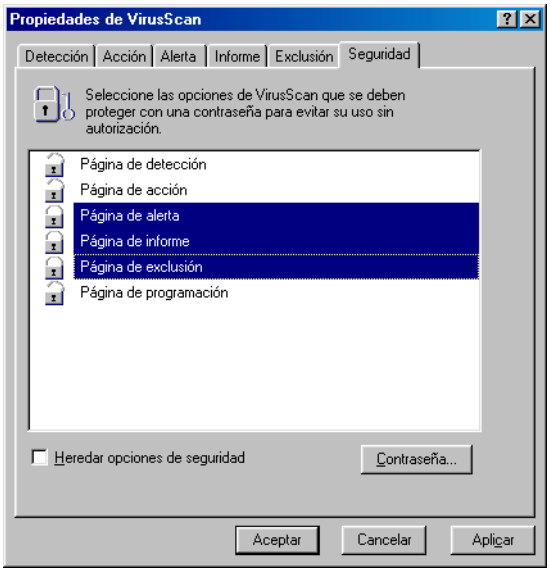

Figura 6-16. Cuadro de diálogo Propiedades de VirusScan: página Seguridad

3. Seleccione la configuración que desee proteger en la lista que aparece.

   Puede proteger una o todas las páginas de propiedades de VirusScan. Las páginas de propiedades protegidas se indican mediante un icono de candado cerrado  que aparece en la lista de seguridad que se muestra en la Figura 6-16. Para eliminar la protección de una página de propiedades, haga clic en el icono de candado cerrado para abrirlo  .

4. Haga clic en **Contraseña** para abrir el cuadro de diálogo Especificar contraseña (Figura 6-17).

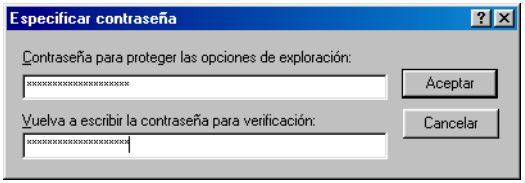

Figura 6-17. Cuadro de diálogo Especificar contraseña

   a. Escriba una contraseña en el primer cuadro de texto que se muestra y, después, vuelva a escribirla en el cuadro de texto que hay debajo del primero para confirmar la selección.

   b. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Especificar contraseña.

5. Para asegurarse de que las opciones de seguridad aparecerán de forma predeterminada en cualquier tarea que cree copiando la tarea pertinente (consulte "Utilización de la ventana de la Consola" en la página 207 para obtener información), active la casilla de verificación **Heredar opciones de seguridad**.

6. Haga clic en una ficha distinta para cambiar cualquiera de las opciones de VirusScan. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo Propiedades de VirusScan, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y volver a la ventana de la Consola. Haga clic en **Cancelar** para volver a la ventana de la Consola sin guardar los cambios.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Uso de herramientas de exploración especializadas 7

Exploración de correo de Microsoft Exchange y Outlook

El software de VirusScan ofrece dos métodos complementarios para proteger el sistema de correo electrónico de Microsoft Exchange o Outlook:

- El explorador VShield incluye un módulo Exploración de correo electrónico que ejecuta operaciones de exploración continuas en segundo plano en el correo electrónico a medida que llega al servidor.
- La extensión Exploración de correo electrónico permite explorar el buzón en el servidor de Exchange si lo desea y en el momento que más le convenga.

La transparente arquitectura de complemento proporciona acceso directo a la extensión Exploración de correo electrónico desde la aplicación de cliente de Exchange u Outlook.

¿Cuándo y por qué debe utilizarse la extensión Exploración de correo electrónico?

La mayoría de los virus, gusanos, y otros agentes hostiles que se propagan con mayor rapidez y que han surgido en los últimos años, se han distribuido por correo electrónico. El correo electrónico ofrece un medio rápido y omnipresente que los creadores de virus pueden utilizar para distribuir los archivos adjuntos infectados, que a menudo engañan a los usuarios para abrirlos y activarlos. Los virus más nuevos, como es el caso de VBS/BUBBLEBOY, pueden incluso funcionar sin que ni siquiera los usuarios tengan que leer o abrir el mensaje de correo electrónico.

Los clientes de correo electrónico de Microsoft Exchange y Outlook son especialmente vulnerables a las infecciones de este tipo debido a las eficaces funciones de interpretación de macros y archivos de comandos. Al igual que con el resto del paquete de aplicaciones de Microsoft Office, el software cliente de Exchange utiliza en gran medida macros, texto marcado, secuencias de comandos y funciones similares que se exponen a los virus.

Utilice el módulo Exploración de correo electrónico de VShield para ejecutar operaciones de exploración en segundo plano en el sistema de correo electrónico y para mantener un nivel constante de vigilancia entre las operaciones de exploración ejecutadas con la extensión Exploración de correo electrónico. En la mayoría de los casos, esto bastará para proteger la integridad del sistema.

Si tiene muchos correos atrasados en el servidor que todavía no ha explorado, si cierra la sesión del servidor de Exchange o si detiene el módulo Exploración de correo electrónico en algún momento, es aconsejable utilizar la extensión Exploración de correo electrónico para explorar el buzón y asegurar de este modo la integridad del sistema. Los virus podrían sencillamente permanecer almacenados en los mensajes de correo electrónico antiguos del servidor o en los mensajes recibidos cuando no esté conectado al sistema de correo electrónico.

Para que las medidas de seguridad antivirus sean fiables, deben incorporar operaciones de exploración completas y periódicas del buzón de correo porque:

- **Una buena seguridad es la mejor protección**. El módulo Exploración de correo electrónico de VShield busca códigos de virus cuando se recibe correo en el servidor o cuando los archivos adjuntos ejecutables se ejecutan después de haberse descargado en el sistema. No obstante, la extensión Exploración de correo electrónico puede explorar el correo antiguo almacenado en el servidor que el módulo Exploración de correo electrónico no percibirá, buscar virus en el correo electrónico que se recibe cuando no se está conectado al servidor de Exchange o explorar el buzón si se ha desactivado temporalmente el módulo Exploración de correo electrónico de VShield.
- **El mantenimiento preventivo es seguridad**. Debido a las rápidas conexiones de correo electrónico del eficaz software cliente con secuencias de comandos y habilitado para Web, el sistema puede infectarse en muy poco tiempo, a veces incluso antes de abrir el correo. Las operaciones de exploración periódicas a menudo interceptan las infecciones antes de que se extiendan o puedan causar algún daño.

Uso de la extensión Exploración de correo electrónico

Para utilizar la extensión Exploración de correo electrónico, debe instalar el software de VirusScan mediante una instalación Personalizada y seleccionar el componente Exploración de correo electrónico (consulte "Pasos de instalación" en la página 40 para obtener más información). Para utilizar la extensión Exploración de correo electrónico con la configuración predeterminada, en primer lugar inicie el software cliente Microsoft Exchange o Microsoft Outlook.

A continuación, siga los siguientes pasos:

1. Conecte con el servidor de correo como lo haría normalmente.
2. Elija la opción **Exploración para detectar virus** en el menú **Herramientas** o haga clic en  en la barra de herramientas de Exchange u Outlook.

   - **NOTA:** Si utiliza Microsoft Exchange 5.0, una limitación en la forma en que el programa actualiza su barra de herramientas impide que aparezcan inmediatamente los botones de la extensión Exploración de correo electrónico. Para agregar el botón Explorar virus a la barra de herramientas, seleccione **Personalizar barra de herramientas** en el menú **Herramientas** y agregue los botones de la extensión Exploración de correo electrónico que aparecen en la lista de botones disponibles del cuadro de diálogo de personalización de barra de herramientas.

   Cuando haya iniciado la extensión Exploración de correo electrónico, comenzará a explorar inmediatamente el buzón de correo de Exchange o Outlook en busca de virus (consulte la Figura 7-1 en la página 244).

   La extensión Exploración de correo electrónico examina de forma predeterminada *todos* los mensajes de correo almacenados en el buzón en el servidor de correo de Exchange en busca de mensajes y archivos adjuntos susceptibles de infectarse con virus. Si tiene muchos mensajes almacenados allí que aún no ha descargado, la operación de exploración llevará mucho tiempo.

   Para hacer una pausa en la operación de exploración, haga clic en  . Para detenerla por completo, haga clic en  . Para reanudarla, haga clic en  .

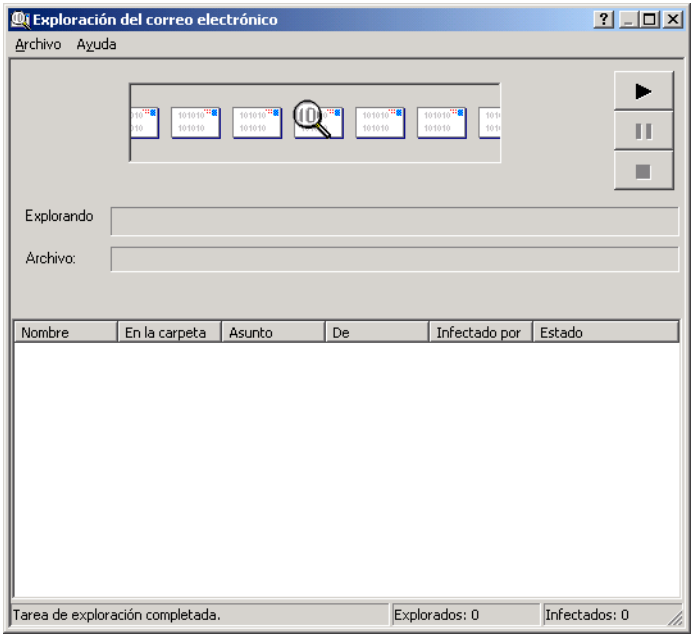

Figura 7-1. Extensión Exploración de correo electrónico en funcionamiento

Si el módulo Exploración de correo electrónico encuentra un archivo infectado, solicitará que le indique cómo responder ante el virus. Consulte "Respuesta cuando la extensión Exploración de correo electrónico detecta un virus" en la página 76 para obtener más información.

Configuración de la extensión Exploración de correo electrónico

La extensión Exploración de correo electrónico está configurada para proteger el sistema en la mayoría de las situaciones y para reaccionar ante los agentes más hostiles que se reciben por correo electrónico. Puede cambiar las opciones de configuración de la extensión para que se adapte mejor a su propio entorno de trabajo. Para cambiar las opciones, debe indicar a la extensión Exploración de correo electrónico:

- qué debe explorar
- qué desea que haga cuando detecte un virus
- cómo debe avisar cuando detecte un virus
- si debe llevar un registro de las acciones

Varias páginas de propiedades en el cuadro de diálogo Propiedades de exploración del correo electrónico contienen opciones para que se ejecute cada operación de exploración. Puede hacer clic en cada ficha para seleccionar las opciones que debe utilizar la extensión para explorar el correo electrónico.

Para que se muestre este cuadro de diálogo, siga los siguientes pasos:

1. Inicie el software cliente de Microsoft Exchange u Outlook y conéctese a su servidor de correo electrónico.

   - **NOTA:** Si ya está conectado al dominio de la red en el que se encuentra su servidor de correo electrónico, es posible que no necesite conectarse directamente el servidor de correo. Bastará con que inicie Exchange u Outlook. Pregunte al administrador de la red cuáles son los requisitos para la conexión al servidor.

2. Seleccione **Propiedades de exploración del correo electrónico** en el menú **Herramientas** o haga clic en en la barra de herramientas de la aplicación cliente.

   Aparecerá el cuadro de diálogo Propiedades de exploración del correo electrónico (Figura 7-2).

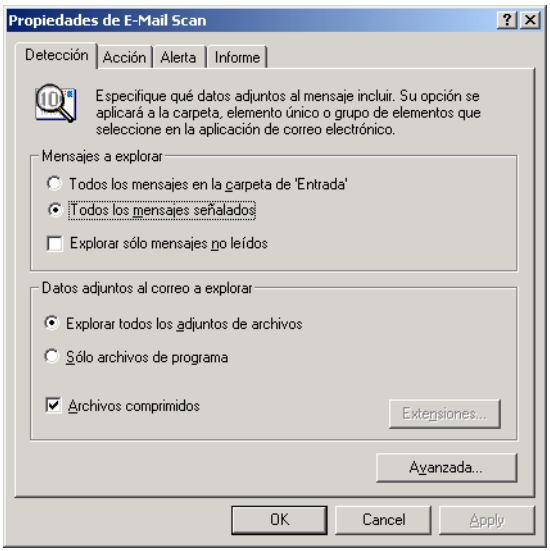

Figura 7-2. Cuadro de diálogo Propiedades de exploración del correo electrónico: página Detección

Selección de las opciones de Detección

Cuando abra por primera vez el cuadro de diálogo Propiedades de exploración del correo electrónico para configurar una operación de exploración, la extensión Exploración de correo electrónico asume que desea explorar todos los mensajes de la Bandeja de entrada, todos los archivos adjuntos en los mensajes, los archivos comprimidos y sólo los archivos susceptibles de infectarse con virus.

De hecho, la extensión Exploración de correo electrónico explora los mensajes de correo electrónico en sí, ya que los archivos de Microsoft Exchange pueden contener macros incrustadas, etiquetas de lenguaje de marcado de hipertexto (HTML), y subprogramas VBScript, que pueden ocultar virus especializados, gusanos o programas de tipo caballo de Troya.

- **NOTA:** La extensión Exploración de correo electrónico se conecta directamente al buzón del servidor de correo de Microsoft Exchange para que se ejecuten las operaciones de exploración. Podrá asimismo explorar cualquier carpeta pública a la que tenga acceso, pero la extensión no explorará los mensajes almacenados en las carpetas personales de Microsoft Outlook (archivos .PST) o elementos almacenados. Sin embargo, los otros componentes de VirusScan explorarán los archivos .PST durante las operaciones de exploración periódicas a menos que los excluya explícitamente.

Para cambiar estas opciones de configuración, complete los siguientes pasos:

1. Seleccione los mensajes de correo electrónico que desee que la extensión Exploración de correo electrónico examine para detectar virus. Puede explorar:

   - **Todos los mensajes en la carpeta de "Entrada"**. Haga clic en este botón para que la extensión detecte virus en los mensajes de correo electrónico almacenados en la Bandeja de entrada de Microsoft Exchange o Microsoft Outlook, independientemente de si los ha leído o no.

     Si tiene almacenado un gran número de mensajes en la Bandeja de entrada, la operación de exploración puede durar mucho tiempo. Sin embargo, si ha instalado la extensión Exploración de correo electrónico después de haber instalado y utilizado el sistema de correo durante un tiempo, McAfee VirusScan Software aconseja que realice al menos una operación de exploración para asegurar que los mensajes de correo antiguos no contienen virus.

- **NOTA:** Una vez que haya descargado el correo en el equipo, el software de VirusScan tratará su carpeta personal o archivo de almacenamiento como lo haría con cualquier otro archivo, a menos que lo excluya específicamente de las operaciones de exploración. De esta forma el nivel de seguridad antivirus es mayor.

- **Todos los mensajes señalados**. Haga clic en este botón para que la extensión busque virus sólo en los mensajes de correo electrónico que seleccione de entre los almacenados en la Bandeja de entrada de Microsoft Exchange o Microsoft Outlook.

2. Para que esta operación de exploración examine sólo los mensajes no leídos, active la casilla de verificación **Explorar sólo mensajes no leídos**. Dependiendo de la opción que seleccione en el Paso 1, la extensión explorará todos los mensajes no leídos del buzón o de las carpetas públicas a las que tenga acceso, o bien los mensajes no leídos que haya seleccionado.

3. Especifique los tipos de archivos que desee que la extensión examine. Podrá:

   - **Explorar archivos comprimidos.** Active la casilla de verificación **Archivos comprimidos** para que la extensión Exploración de correo electrónico busque virus en los archivos comprimidos y archivos de almacenamiento. Aunque esta opción proporciona mayor protección, la exploración de archivos comprimidos puede aumentar la cantidad de tiempo necesario para las operaciones de exploración.

     La extensión explora los mismos tipos de archivos comprimidos y archivos de almacenamiento que la aplicación VirusScan. Para ver una lista de los archivos y los archivos de almacenamiento, consulte "Lista actual de archivos comprimidos explorados" en la página 293.

   - **Explorar todos los archivos**. Active la casilla de verificación **Todos los archivos** para que la extensión Exploración de correo electrónico explore todos los tipos de archivos del buzón, independientemente de las extensiones del nombre de archivo.

     - **NOTA:** McAfee VirusScan Software recomienda que seleccione esta opción la primera vez que realice una exploración y periódicamente en futuras ocasiones, para asegurarse de que el buzón no contiene virus. De este modo, puede limitar el ámbito de operaciones de exploración posteriores.

- **Seleccionar los tipos de archivos**. Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea archivos de comandos, macros o códigos binarios. Por tanto, podrá reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, limitándolo a los archivos con mayores probabilidades de ser infectados. Para ello, haga clic en el botón **Sólo archivos de programa**.

  Para ver o designar los tipos de archivos que la extensión Exploración de correo electrónico va a examinar, haga clic en **Extensiones**. De este modo se abre el cuadro de diálogo Extensiones de archivos de programa. Para obtener información sobre cómo cambiar los archivos de la lista, consulte "Agregar extensiones de nombre de archivo para explorar" en la página 287.

4. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración (Figura 7-3).

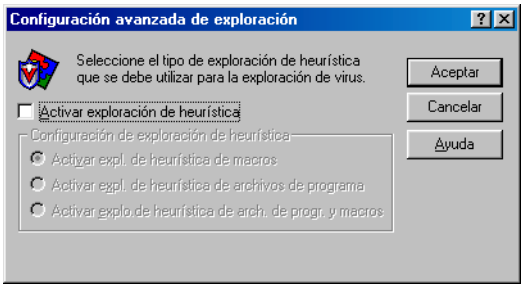

Figura 7-3. Cuadro de diálogo Configuración avanzada de exploración

La tecnología de exploración heurística permite a la extensión Exploración de correo electrónico reconocer nuevos virus basándose en su parecido a virus similares que el módulo ya conoce. Para hacerlo, la extensión busca determinadas características "tipo virus" en los archivos especificados para explorar. La presencia de una cantidad suficiente de estas características en un archivo lleva a la extensión a identificarlo como posiblemente infectado con un nuevo virus o con uno previamente no identificado.

Puesto que la extensión busca simultáneamente características en el archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas de infección. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

La extensión Exploración de correo electrónico se inicia sin las opciones de exploración heurística activas. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que desee que la extensión Exploración de correo electrónico utilice. Podrá elegir entre las siguientes opciones:

   – **Activar expl. de heurística de macros**. Seleccione esta opción para que la extensión identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que incluyan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. La extensión identificará las coincidencias totales con el nombre del virus correspondiente. Cuando las firmas del código recuerden a virus existentes, dicha aplicación indicará que ha encontrado un posible virus de macro.

   – **Activar expl. de heurística de arch. de programa.** Seleccione esta opción para que la extensión Exploración de correo electrónico localice nuevos virus en archivos de programa examinando sus características y comparándolas con una lista de características de virus conocidos. La extensión identificará los archivos que tengan un número suficiente de estas características como posibles virus.

   – **Activar expl. de heurística de arch. de programa y macros.** Seleccione esta opción para que la extensión utilice ambos tipos de exploración heurística. McAfee VirusScan Software aconseja el uso de esta opción para obtener una protección antivirus total.

   • **NOTA:** la extensión utilizará técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide examinar **Todos los archivos**, utilizará una exploración heurística para todos los tipos de archivos.

   ---

c. Haga clic en **Aceptar** para guardar los cambios y volver al cuadro de diálogo Propiedades de exploración del correo electrónico.

5. Haga clic en la ficha Acción para seleccionar otras opciones de la extensión Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de Propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Acción

Cuando la extensión Exploración de correo electrónico detecta un virus, puede responder preguntando qué debe hacer con el archivo infectado o emprender automáticamente la acción que se le haya indicado de antemano. Utilice la página de propiedades Acción para especificar qué opciones de respuesta desea que la extensión le ofrezca cuando encuentre un virus, o qué acciones desea que emprenda automáticamente.

Siga estos pasos:

1. Haga clic en el cuadro de diálogo Propiedades de exploración del correo electrónico para mostrar la página de propiedades adecuada (Figura 7-4).

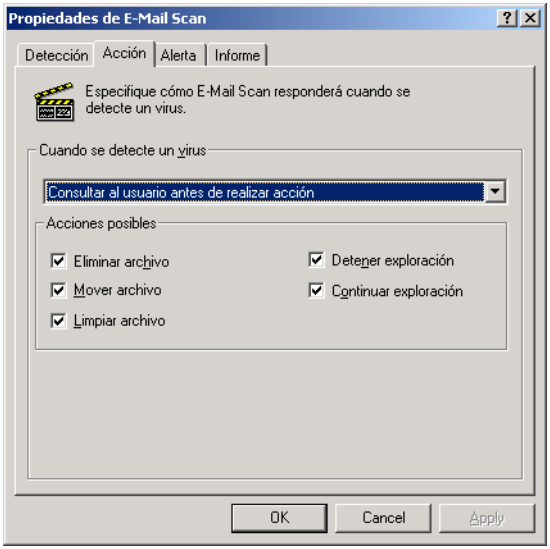

Figura 7-4. Cuadro de diálogo Propiedades de exploración del correo electrónico: página Acción

2. Elija una respuesta en la lista **Cuando se encuentre un virus**. El área situada inmediatamente debajo de la lista cambiará para mostrar opciones adicionales para cada respuesta.

   Podrá elegir entre las siguientes opciones:

   - **Consultar al usuario antes de realizar acción.** Elija esta respuesta si espera estar trabajando con el ordenador cuando la extensión Exploración del correo electrónico examine el buzón. El programa presentará mensajes de alerta cuando encuentre un virus y le ofrecerá una gama de posibles respuestas.

     Cada casilla de verificación que se active en la página Acción hace que aparezca un botón en el mensaje de alerta que la extensión muestra cuando encuentra un virus. Por ejemplo, al seleccionar **Eliminar archivo**, aparecerá el botón **Eliminar** en el mensaje de alerta.

     Puede seleccionar una de las siguientes opciones:

     – **Limpiar archivo**. Esta opción indica a la extensión que intente eliminar el código de virus del archivo infectado. Si la función de elaboración de informes está activada, grabará un suceso de registro cada vez que limpie o no pueda limpiar un archivo infectado.

     – **Eliminar archivo**. Esta opción indica a la extensión que elimine inmediatamente el archivo infectado.

     – **Mover archivo**. Esta opción indica a la extensión que desplace el archivo infectado a una carpeta de cuarentena. El mensaje de alerta mostrará un botón **Mover archivo a** que permite enviar el elemento infectado a una carpeta de cuarentena en el servidor de Microsoft Exchange. Podrá mover los elementos infectados a cualquier otra carpeta que haya creado en el buzón de Outlook o Exchange, o bien a cualquier carpeta pública en el servidor de Exchange a la que tenga acceso. El elemento permanecerá en el servidor de Exchange hasta que lo elimine; no se descargará en el equipo.

     – **Continuar la exploración**. Esta opción indica a la extensión que continúe con la exploración, pero que no emprenda ninguna otra acción. Si las opciones de generación de informes están activadas, la extensión incluirá el incidente en su archivo de registro.

  - **Detener exploración**. Esta opción indica a la extensión que detenga inmediatamente la operación de exploración. Si desea continuar, debe hacer clic de nuevo en  en la barra de herramientas de Outlook o Exchange, o bien seleccione **Exploración para detectar virus** en el menú **Herramientas** para reiniciar la operación.

- **Mover archivos infectados automáticamente**. Seleccione esta respuesta para que la extensión mueva los archivos infectados a una carpeta de cuarentena en el servidor de Microsoft Exchange tan pronto como los detecte. La extensión mueve estos archivos a una carpeta denominada Infectados, ubicada en el servidor de Microsoft Exchange.
- **Limpiar los archivos infectados automáticamente**. Seleccione esta respuesta para indicar a la extensión que elimine el código de virus del archivo adjunto infectado tan pronto como lo detecte. Si la extensión no puede eliminar el virus, anotará el incidente en el archivo de registro.
- **Eliminar los archivos infectados automáticamente**. Seleccione esta opción para que la extensión elimine inmediatamente todos los archivos adjuntos de correo electrónico infectados que detecte. Asegúrese de activar la función de generación de informes para poder tener un registro de todos los archivos que la extensión haya eliminado. Si la extensión no puede eliminar el archivo infectado, anotará el incidente en el archivo de registro.
- **Continuar la exploración**. Utilice esta opción sólo si prevé dejar el equipo sin atención mientras la aplicación comprueba si hay virus. Si también activa la función de generación de informes, la aplicación registrará los nombres de los virus que encuentre y de los archivos infectados para que los elimine tan pronto como tenga la oportunidad.

+ **ADVERTENCIA:** La extensión Exploración de correo electrónico *no* intentará romper ningún mensaje codificado para explorarlos. Si un archivo adjunto infectado contiene una firma digital, la extensión *eliminará* la firma digital para limpiar o eliminar el archivo infectado.

---

3. Haga clic en la ficha Alerta para seleccionar otras opciones de la extensión Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de Propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Alerta

Tras configurar las opciones de repuesta deseadas, podrá configurar la extensión Exploración de correo electrónico para que busque y elimine automáticamente virus del buzón de Exchange, cuando los detecte, sin casi ninguna intervención posterior. Para que la extensión le informe inmediatamente de que ha encontrado un virus de modo que pueda tomar las medidas apropiadas, es necesario configurarla para que envíe un mensaje de alerta.

Siga estos pasos:

1. Haga clic en la ficha Alerta del cuadro de diálogo Propiedades de exploración del correo electrónico para mostrar la página de propiedades adecuada (Figura 7-5).

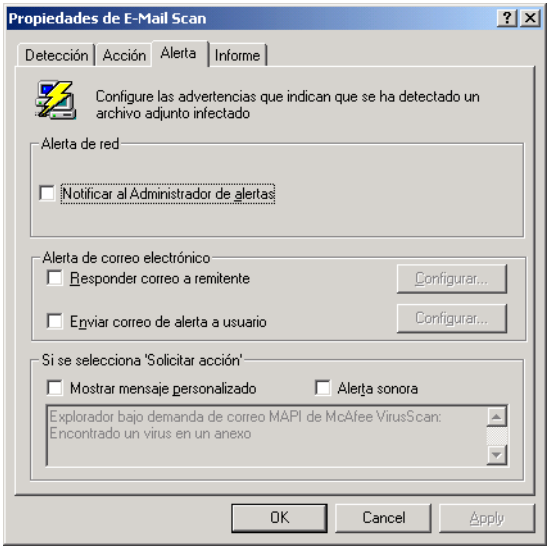

Figura 7-5. Cuadro de diálogo Propiedades de exploración del correo electrónico: página Alerta.

2. Active la casilla de verificación **Notificar al Administrador de alertas** para que la extensión Exploración de correo electrónico envíe mensajes de alerta al Administrador de alertas para su distribución.

El Administrador de alertas es un componente de software independiente de McAfee VirusScan que reúne mensajes de alerta y utiliza varios métodos para enviarlos a los destinatarios que especifique. Para que la extensión envíe satisfactoriamente estos mensajes de alerta, debe configurar la utilidad de configuración de cliente del Administrador de alertas. Consulte "Utilización de la utilidad de configuración de cliente del Administrador de alertas" en la página 270 para obtener más información.

Podrá enviar directamente mensajes de alerta a un servidor del Administrador de alertas, o bien enviar los mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas comprueba periódicamente.

- **NOTA**: Si desactiva esta casilla de verificación indicará a la extensión Exploración de correo electrónico que no envíe un mensaje de alerta mediante el Administrador de alertas, sin embargo, esto no afecta a otros mensajes de alerta configurados en esta página de propiedades.

Como parte del sistema de advertencia del antivirus, la extensión Exploración de correo electrónico puede responder directamente con un mensaje de alerta a cualquier persona que envíe un mensaje o archivo adjunto infectado. Puede copiar ese mensaje y enviarlo a otros destinatarios, dentro y fuera de su empresa.

Si prefiere no enviar una respuesta, podrá simplemente hacer que la extensión envíe una notificación de correo electrónico, quizás a un administrador del sistema, cada vez que detecte un virus.

El envío de mensajes de respuesta podrá servir para detectar las fuentes de los virus y determinar por dónde se introducen los agentes infecciosos en la red. El envío de copias de estos mensajes a los administradores del sistema puede ayudarles a realizar un seguimiento de la propagación de las infecciones.

También puede optar por enviar mensajes a cualquier destinatario sin responder al emisor del archivo adjunto infectado. La extensión Exploración de correo electrónico puede obtener los destinatarios directamente de la libreta de direcciones de Microsoft Exchange, Microsoft Outlook, de otras compatibles con MAPI o de cualquier directorio Lotus cc:Mail equivalente. También puede introducir directamente las direcciones de los destinatarios.

El mensaje que cree para las respuestas es una plantilla. La extensión Exploración de correo electrónico enviará el mensaje que escriba automáticamente a cada destinatario que designe, por lo que McAfee VirusScan recomienda escribir un mensaje que todos los destinatarios puedan leer y entender. Aparte de los pasos que debe realizar para escribir el mensaje de la plantilla, la extensión no le dará la oportunidad de modificar el mensaje antes de enviarlo.

Puede enviar un mensaje para responder al emisor del mensaje infectado y otro diferente al resto de destinatarios, pero no podrá adaptar el mismo mensaje para distintos destinatarios.

3. Para elaborar los mensajes de plantilla, siga los siguientes pasos:

   a. Active la casilla de verificación **Responder correo a remitente** en la página de propiedades Alerta y, a continuación, haga clic en **Configurar** para abrir un formulario de mensaje de correo estándar.

      Como la extensión Exploración de correo electrónico devolverá este mensaje directamente al emisor del mensaje de correo electrónico infectado, el botón **Para:** y el cuadro de texto no estarán disponibles.

   b. Para enviar una copia de este mensaje a otra persona, escriba su dirección de correo electrónico en el cuadro de texto Cc:, o bien haga clic en **Cc:** para elegir un destinatario en la libreta de direcciones o el directorio del usuario del sistema de correo electrónico.

      - **NOTA:** Para buscar una dirección de correo electrónico en el directorio del usuario del sistema de correo electrónico, deberá almacenar la información con las direcciones en un directorio del usuario, base de datos o libreta de direcciones compatibles con MAPI, o bien en un directorio Lotus cc:Mail equivalente. Si aún no ha entrado en el sistema de correo electrónico, la extensión Exploración de correo electrónico tratará de utilizar el perfil MAPI predeterminado para entrar en sistemas de correo compatibles con MAPI, o le solicitará el nombre de usuario, la contraseña y la ruta de acceso al buzón de Lotus cc:Mail. Escriba la dirección que solicite la extensión y, a continuación, haga clic en **Aceptar** para continuar.

      ---

   c. Especifique un asunto en el mensaje que refleje la importancia del mismo y agregue algún comentario en el cuerpo del mensaje, debajo de una notificación de virus estándar que facilitará la propia extensión. Puede añadir hasta 1.024 caracteres de texto.

d. Haga clic en **Aceptar** para guardar el mensaje.

Siempre que detecte un virus, la extensión enviará una copia de este mensaje a todas las personas que le envíen correo con un archivo adjunto infectado. El programa tomará la dirección del destinatario de la información encontrada en la cabecera del mensaje original e identificará el virus y el archivo afectado en el área que se encuentra justo debajo de la línea de asunto. Además, si tiene activada la función de generación de informes, la extensión también registrará cada incidente cuando envíe un mensaje de alerta.

e. Para enviar un mensaje de correo electrónico con el fin de advertir a otros usuarios de un archivo adjunto infectado, por ejemplo, a un administrador de red, active la casilla de verificación **Enviar correo de alerta a usuario** en la página de propiedades Alerta. Podrá escribir una respuesta estándar del mismo modo que lo hizo desde el Paso a al Paso d. Sin embargo, en este caso podrá rellenar los cuadros de texto Para: y Cc:.

Siempre que detecte un virus, la extensión Exploración de correo electrónico enviará una copia de este mensaje a todas las direcciones que escriba para el mismo.

4. Active la casilla de verificación **Alerta sonora** para que la extensión emita un sonido cuando encuentre un archivo infectado.

Puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. De lo contrario, la casilla de verificación mostrará y utilizará la configuración que tenía la última vez que seleccionó el elemento **Consultar al usuario antes de realizar acción**.

La extensión emitirá un sonido estándar de alerta del sistema o el archivo .WAV que tenga configurado el equipo.

5. Active la casilla de verificación **Mostrar mensaje personalizado** para que la extensión agregue un mensaje personalizado al cuadro de alerta que aparece cada vez que encuentra un archivo infectado.

Del mismo modo que ocurre con la alerta sonora, puede cambiar la configuración de esta opción sólo con seleccionar **Consultar al usuario antes de realizar acción** en la página de propiedades Acción. Si no selecciona este elemento en la página Acción, no aparecerá ningún cuadro de alertas ni verá ningún mensaje personalizado aunque active esta casilla de verificación.

6. Escriba el mensaje que desee que la extensión muestre en el cuadro de texto proporcionado. Puede escribir 250 caracteres como máximo.

7. Haga clic en la ficha Informe para seleccionar otras opciones de la extensión Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de Propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

   - **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Selección de las opciones de Informe

La extensión Exploración de correo electrónico muestra la configuración actual y resume todas las acciones que emprende durante las operaciones de exploración en un archivo de registro denominado MAILSCAN.TXT. Puede hacer que la extensión escriba su registro en este archivo o podrá utilizar cualquier editor de texto para crear un archivo de texto con el fin de lo que lo utilice la extensión. Después podrá abrir e imprimir el archivo de registro para examinarlo desde la extensión Exploración de correo electrónico o desde un editor de texto.

Puede utilizar el archivo MAILSCAN.TXT para realizar un seguimiento de la actividad del virus en el sistema y saber las opciones que ha utilizado la extensión para detectar y reaccionar ante los virus que ha detectado. También podrá utilizar los informes de incidentes registrados en el archivo para determinar qué archivos debe examinar en cuarentena o cuáles debe eliminar del equipo.

Para hacer que la extensión anote sus acciones en un archivo de registro, realice las siguientes operaciones:

1. Haga clic en la ficha Informe del cuadro de diálogo Propiedades de exploración del correo electrónico para mostrar la página de propiedades adecuada (Figura 7-6 en la página 258).

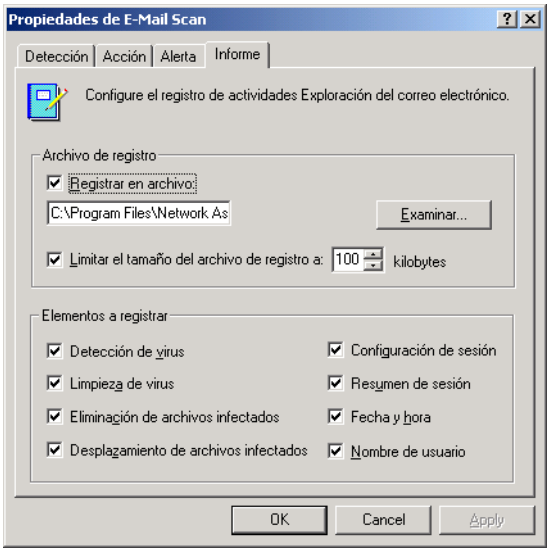

Figura 7-6. Cuadro de diálogo Propiedades de exploración del correo electrónico: página Informe

2. Active la casilla de verificación **Registrar en archivo**.

   Como opción predeterminada, la extensión Exploración de correo electrónico escribe la información de registro en el archivo MAILSCAN.TXT, en el directorio de programa de VirusScan. Puede escribir un nombre distinto en el cuadro de texto correspondiente, o hacer clic en **Examinar** para encontrar un archivo adecuado en su disco duro o en la red. Puede utilizar un archivo diferente, pero debe existir el archivo de texto. La extensión no creará un archivo nuevo.

   - **NOTA:** Si selecciona una ubicación distinta para el archivo de registro en un sistema Windows NT Workstation versión 4.0 o Windows 2000 Professional, asegúrese de que selecciona una ubicación a la que tenga acceso a nivel de usuario. Dado que la extensión Exploración de correo electrónico se ejecuta con los mismos derechos de acceso que el programa cliente de correo electrónico, no podrá escribir correctamente en un archivo de registro si la ubicación del archivo requiere derechos de acceso de Administrador y ha entrado como usuario para ejecutar el programa cliente de correo electrónico. La extensión Exploración de correo electrónico mostrará entonces un mensaje "Error de acceso al registro de actividades" cuando detecte un virus.

3. Para reducir el tamaño del archivo de registro, active la casilla de verificación **Limitar el tamaño del archivo de registro a** y, a continuación, escriba un valor para el tamaño del archivo, en kilobytes, en el cuadro de texto correspondiente. Si no activa esta casilla de verificación, el tamaño del archivo de registro puede aumentar tanto como el espacio en disco lo permita.

   Escriba un valor entre 10 KB y 999 KB. Como opción predeterminada, la extensión limita el tamaño del archivo a 100 KB. Si los datos registrados sobrepasan el tamaño de archivo especificado, la extensión eliminará el registro existente y comenzará de nuevo desde el punto en el que se quedó.

4. Active las casillas de verificación que correspondan a la información que desea que la extensión incluya en el archivo de registro. Cada casilla de verificación que se selecciona aquí hace que la extensión registre esa información, normalmente cuando la exploración finaliza, o cuando el usuario apaga el sistema:

   - **Detección de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que la extensión encuentre durante cada operación de exploración. Desactive la casilla de verificación para no incluir esta información en el archivo de registro.
   - **Limpieza de virus**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que la extensión limpie o intente limpiar durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
   - **Eliminación de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que la extensión elimine durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
   - **Desplazamiento de archivos infectados**. Active esta casilla de verificación para que el archivo de registro incluya el número de virus que la extensión mueva a una carpeta de cuarentena durante cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
   - **Configuración de sesión**. Active esta casilla de verificación para que el archivo de registro incluya las opciones de configuración utilizadas por la extensión durante cada operación de configuración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

- **Resumen de sesión**. Active esta casilla de verificación para que el archivo de registro haga un resumen de las acciones que la extensión realizó durante cada operación de exploración. El registro incluirá:
  - Número de archivos que la extensión ha examinado.
  - Número de archivos infectados que la extensión ha limpiado.
  - Número de archivos infectados que la extensión ha eliminado.
  - Número de archivos infectados que la extensión ha movido a una carpeta de cuarentena.
  - Las opciones de configuración de la extensión.

  Desactive la casilla de verificación para no incluir esta información en el archivo de registro.
- **Fecha y hora**. Active esta casilla de verificación para que el archivo de registro incluya la fecha y la hora a la que la extensión comenzó la operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.
- **Nombre de usuario**. Active esta casilla de verificación para que el archivo de registro incluya el nombre de usuario registrado en la estación de trabajo cuando la extensión inicie cada operación de exploración. Desactive esta casilla de verificación para no incluir esta información en el archivo de registro.

5. Haga clic en una ficha distinta para cambiar cualquiera de las opciones de configuración de la extensión Exploración de correo electrónico. Para guardar los cambios efectuados sin cerrar el cuadro de diálogo de Propiedades de exploración del correo electrónico, haga clic en **Aplicar**. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA:** Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

Exploración de cc:Mail

El software de VirusScan incluye soporte original para clientes de Microsoft Exchange y Outlook, así como para Lotus cc:Mail v6.0, v7.0 y v8.0. Los clientes de cc:Mail utilizan un sistema de corre electrónico patentado que la extensión Exploración de correo electrónico no puede utilizar directamente. El software de VirusScan incluye una extensión especializada de cc:Mail que complementa el software de VShield, entra en el sistema cc:Mail y, a continuación, examina el correo nuevo de la Bandeja de entrada de cc: Mail mientras funciona discretamente en segundo plano. Cuando llegan mensajes nuevos, el explorador de cc:Mail los examina para localizar archivos adjuntos infectados antes de que el software cliente los descargue al equipo.

La única interacción real del usuario con Exploración de cc:Mail se produce cuando selecciona el sistema de correo electrónico corporativo que el explorador VShield utilizará para buscar virus. Para obtener información sobre cómo especificar cc:Mail como sistema corporativo de correo electrónico, consulte "Selección de las opciones de Detección" en la página 123.

Si aún no se ha conectado al servidor de cc:Mail, el explorador de cc:Mail podría solicitarle que introduzca su nombre de usuario y contraseña en una pantalla de conexión para que pueda acceder al servidor de cc:Mail y explorar la Bandeja de entrada. Escriba su nombre de usuario y su contraseña para cc:Mail, como si fuera a conectarse directamente a cc:Mail y haga clic en **Aceptar** para continuar. Después, inicie su aplicación cliente de cc:Mail y establezca el intervalo de tiempo (superior a cinco minutos) para que el cliente examine el servidor de cc: Mail. De esta forma, el software de VShield podrá examinar el correo antes de que el software cliente lo recupere.

El componente cc:Mail se desconectará del servidor de correo electrónico cuando salga del software cliente.

Uso de la utilidad ScreenScan

La utilidad ScreenScan explora el sistema en segundo plano mientras se ejecuta el protector de pantalla. De esta forma, puede transformar los períodos de inactividad en productivos si permite que la máquina compruebe por sí misma si existen virus en el sistema. ScreenScan no emprende ninguna acción contra los virus que detecta, pero anota los resultados de sus operaciones de exploración en un archivo de registro que puede revisar cuando lo crea conveniente.

- **NOTA:** Para utilizar ScreenScan, debe seleccionar la instalación Personalizada durante Instalación. La utilidad Setup, de forma predeterminada, no instalará este componente. Consulte "Pasos de instalación" en la página 40 para obtener más información.

Una vez instalado, ScreenScan muestra una página de propiedades en el cuadro de diálogo de propiedades de pantalla de Windows. En él puede seleccionar las opciones de detección e informe que desee que utilice ScreenScan.

Siempre que la haya configurado y activado, la utilidad se iniciará cuando el protector de pantalla del equipo se active, y se detendrá cuando mueva el ratón, presione una tecla en el teclado, o realice cualquier otra acción que interrumpa el protector de pantalla.

Para configurar ScreenScan, realice los siguientes pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.
2. En la ventana que aparece, localice y haga doble clic en Pantalla para abrir el cuadro de diálogo Propiedades de Pantalla. A continuación, haga clic en la ficha ScreenScan (Figura 7-7).

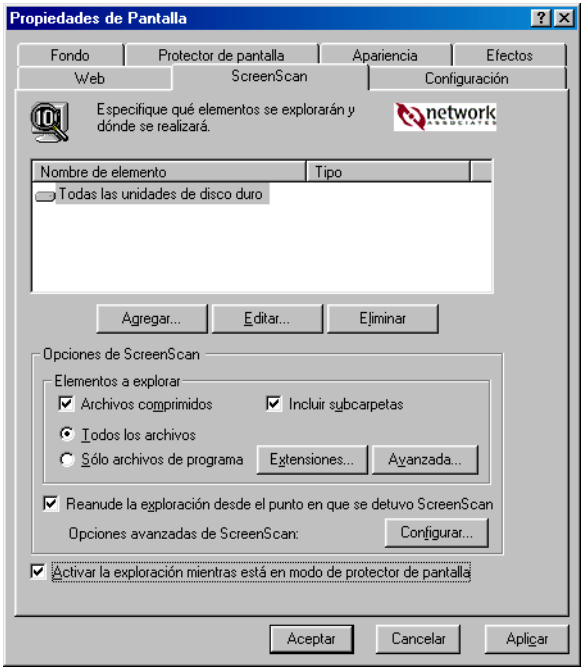

Figura 7-7. Cuadro de diálogo Propiedades de Pantalla: página ScreenScan

3. Active la casilla de verificación **Activar exploración mientras está en modo de protector de pantalla** para activar las opciones del resto de la página de propiedades.

4. Seleccione las partes del sistema que desee que la utilidad ScreenScan examine para buscar virus. Podrá:

   - **Agregar objetivos de exploración.** Haga clic en **Agregar** para abrir el cuadro de diálogo Agregar elemento de exploración (vea la Figura 7-8).

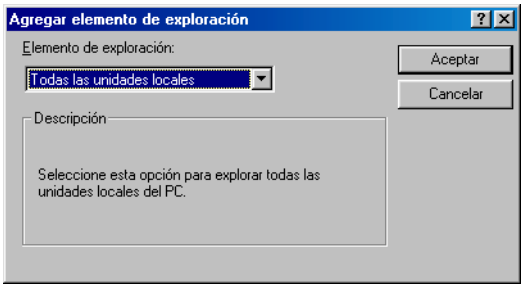

Figura 7-8. Cuadro de diálogo Agregar elemento de exploración

A continuación, seleccione el objetivo de exploración de la lista que se facilita. Podrá elegir entre las siguientes opciones:

- **Todas las unidades locales**. De este modo indicará a la utilidad que explore todas las unidades conectadas físicamente al equipo, incluidas las unidades de medios extraíbles.
- **Unidad o carpeta**. De este modo indicará a la utilidad que explore determinados archivos o carpetas del sistema. Escriba en el cuadro de texto correspondiente la letra de unidad o la ruta de acceso a la carpeta que desea explorar, o haga clic en **Examinar** para buscar el objetivo de exploración en el equipo.
- **Todas las unidades de disco duro**. Indica a la utilidad que explore los discos duros que estén conectados físicamente al equipo.

Cuando haya seleccionado el destino, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Cambiar objetivos de exploración.** Seleccione uno de los objetivos de exploración detallados y haga clic en **Editar** para abrir el cuadro de diálogo Editar elemento de exploración (Figura 7-9).

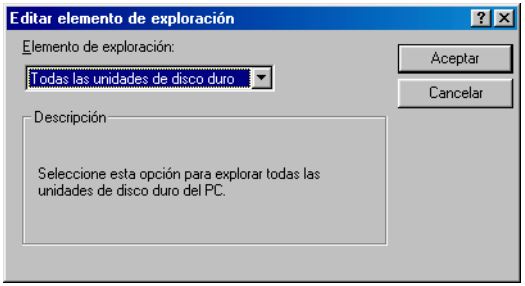

Figura 7-9. Cuadro de diálogo Editar elemento de exploración

En el cuadro de diálogo aparecerá seleccionado el objetivo de exploración existente. Seleccione o escriba un nuevo objetivo de exploración y, a continuación, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Eliminar objetivos de exploración.** Seleccione uno de los objetivos de exploración detallados y haga clic en **Eliminar** para eliminarlo.

5. Especifique los tipos de archivos que desea que examine la utilidad ScreenScan. Podrá:

   - **Explorar archivos comprimidos**. Active la casilla de verificación **Archivos comprimidos** para que la utilidad busque virus en archivos comprimidos o en archivos de almacenamiento. Para ver una lista de los tipos de archivos que explora la aplicación, consulte "Lista actual de archivos comprimidos explorados" en la página 293.

   - **Explorar subcarpetas dentro del objetivo especificado**. Active la casilla de verificación**Incluir subcarpetas** para que la utilidad busque virus en cualquier carpeta en el objetivo de exploración.

     - **NOTA:** Al seleccionar **Incluir subcarpetas** la utilidad realiza una exploración sólo en aquellos archivos almacenados en las propias subcarpetas. La utilidad no explorará los archivos almacenados en el directorio raíz de la carpeta que indique. Para explorar esos archivos, desactive la casilla de verificación **Incluir subcarpetas**.

- **Explorar todos los archivos**. Active la casilla de verificación **Todos los archivos** para que la utilidad explore todos los archivos del buzón o carpeta pública que haya especificado sea cual sea la extensión.

  - **NOTA:** McAfee VirusScan Software recomienda que seleccione esta opción la primera vez que realice una exploración y periódicamente en futuras ocasiones, para asegurarse de que el sistema no contiene virus. De este modo, puede limitar el ámbito de operaciones de exploración posteriores.

- **Seleccionar los tipos de archivos**. Los virus no podrán infectar archivos que contengan código no ejecutable, ya sea archivos de comandos, macros o códigos binarios. Por tanto, podrá reducir el ámbito de las operaciones de exploración, sin riesgo para la seguridad, limitándolo a los archivos con mayores probabilidades de ser infectados. Para ello, haga clic en el botón **Sólo archivos de programa**.

  Para ver o designar las extensiones de nombres de archivo que la utilidad ScreenScan examinará, haga clic en **Extensiones**. De este modo se abre el cuadro de diálogo Extensiones de archivos de programa. Para obtener información sobre cómo cambiar los archivos de la lista, consulte "Agregar extensiones de nombre de archivo para explorar" en la página 287.

6. Active la exploración de heurística. Haga clic en **Avanzada** para abrir el cuadro de diálogo Configuración avanzada de exploración (consulte la Figura 7-10).

   La tecnología de exploración heurística permite a la utilidad ScreenScan reconocer nuevos virus basándose en su parecido a virus similares que el módulo ya conoce. Para hacerlo, la utilidad busca determinadas características "tipo virus" en los archivos especificados para explorar.

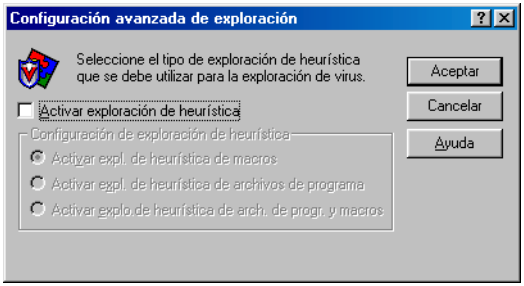

Figura 7-10. Cuadro de diálogo Configuración avanzada de exploración

La presencia de una cantidad suficiente de estas características en un archivo lleva a la utilidad a identificarlo como posiblemente infectado con un nuevo virus o con uno previamente no identificado.

Puesto que la utilidad busca simultáneamente características de archivo que descarten la posibilidad de una infección por virus, en muy pocas ocasiones le hará llegar falsas alarmas de infección. Por lo tanto, a menos que sepa que el archivo *no* contiene virus, deberá tratar las infecciones "potenciales" con la misma cautela que cuando se trata de infecciones confirmadas.

La utilidad ScreenScan se inicia sin ninguna opción de exploración heurística activa. Para activar la exploración heurística, siga estos pasos:

a. Active la casilla de verificación **Activar exploración de heurística**. Las demás opciones del cuadro de diálogo se activarán.

b. Seleccione los tipos de exploración heurística que desee que la utilidad ScreenScan utilice. Podrá elegir entre las siguientes opciones:

   – **Activar expl. de heurística de macros**. Seleccione esta opción para que la utilidad identifique todos los archivos de Microsoft Word, Microsoft Excel y otros archivos de Microsoft Office que incluyan macros incrustadas, para después comparar el código de esas macros con su base de datos de definiciones de virus. La utilidad identificará las coincidencias totales con el nombre del virus correspondiente. Cuando las firmas del código recuerden a virus existentes, dicha utilidad indicará que ha encontrado un posible virus en una macro.

– **Activar expl. de heurística de arch. de programa.** Seleccione esta opción para que la utilidad ScreenScan localice nuevos virus en archivos de programa examinando sus características y comparándolas con una lista de características de virus conocidos. La utilidad identificará los archivos que tengan un número suficiente de estas características como posibles virus.

– **Activar expl. de heurística de arch. de programa y macros.** Seleccione esta opción para que la utilidad utilice ambos tipos de exploración heurística. McAfee VirusScan Software aconseja el uso de esta opción para obtener una protección antivirus total.

• **NOTA:** La utilidad utilizará técnicas de exploración heurística sólo en los tipos de archivo designados en el cuadro de diálogo Extensiones de archivos de programa. Si decide examinar **Todos los archivos**, utilizará una exploración heurística para todos los tipos de archivos.

---

7. Configure la utilidad ScreenScan para que reanude cualquier operación de exploración en el momento en que se detuvo. Active **Reanude la exploración desde el punto en que se detuvo ScreenScan**.

   Si no activa esta casilla de verificación, la utilidad reanudará la operación de exploración desde el directorio raíz de la primera unidad que especificó como objetivo de exploración, cada vez que el protector de pantalla se ejecute. De este modo la utilidad podría explorar algunas partes del sistema varias veces mientras que omitiría otras.

8. Configure las opciones avanzadas de ScreenScan. Haga clic en **Configurar** para abrir el cuadro de diálogo Configuración avanzada del explorador (Figura 7-11).

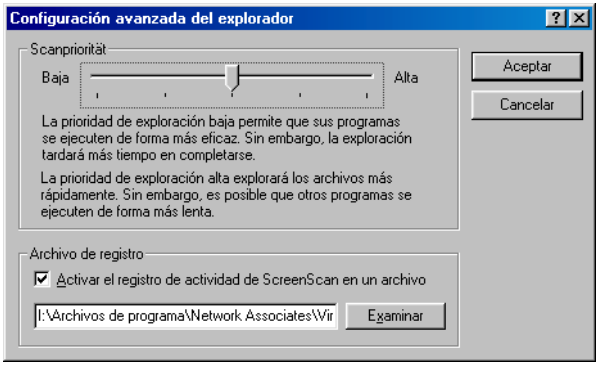

Figura 7-11. Cuadro de diálogo Configuración avanzada del explorador

Podrá elegir entre las siguientes opciones:

- **Establecer una prioridad de ejecución para las tareas de ScreenScan**. Establezca el control de prioridad de exploración en **Alta** para otorgar una prioridad mayor a los recursos y tiempo del sistema de la utilidad ScreenScan, que a otras actividades realizadas en segundo plano, como las operaciones de desfragmentación, que se llevan a cabo durante los períodos de inactividad del equipo. Esto hace que otras actividades se ejecuten de forma más lenta.

  Establezca el control en **Baja** para otorgar a las tareas en segundo plano mayor prioridad que a la utilidad ScreenScan. Con esto consigue que la utilidad ScreenScan se ejecute de forma más lenta.

- **Indicar a la utilidad que registre las acciones**. Active la casilla de verificación **Activar el registro de actividad de ScrenScan en un archivo** para que la utilidad ScreenScan mientras se ejecuta, refleje las acciones que realiza en el archivo SCREENSCAN ACTIVITY LOG.TXT.

  La utilidad registrará las acciones cuando detenga la tarea o cuando apague el sistema. Si prefiere registrar los datos en un archivo de texto diferente, escriba la ruta y el nombre de archivo en el cuadro de texto proporcionado, o haga clic en **Examinar** para ubicar el archivo. La utilidad ScreenScan no generará un archivo de texto, escribirá sólo en un archivo existente.

9. Haga clic en **Aplicar** para guardar los cambios sin cerrar el cuadro de diálogo Propiedades de Pantalla. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en **Cancelar** para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

- **NOTA**: Al hacer clic en **Cancelar** no se anularán los cambios que ya se hayan guardado al hacer clic en **Aplicar**.

La utilidad ScreenScan se ejecutará la próxima vez que lo haga el protector de pantalla. Si cambia los protectores de pantalla, también tendrá que volver a configurar la opciones de la utilidad ScreenScan.

Utilización de las utilidades de VirusScan 8

Descripción del panel de control de VirusScan

El panel de control de VirusScan constituye la interfaz gráfica del servicio de administración de VirusScan, que inicia y controla todos los procesos de los principales componentes, incluidos la aplicación VirusScan, la Consola y el explorador VShield. El servicio de administración de VirusScan también proporciona una estructura de memoria común para todos los componentes de VirusScan, que les permite compartir datos y actuar sobre ellos.

A efectos prácticos, puede utilizar el panel de control para:

- Iniciar y detener todos los componentes de VirusScan con un solo botón
- Indicar al explorador VShield y a la Consola de VirusScan que se carguen tan pronto como se inicie el equipo
- Definir el número máximo de objetivos que la aplicación VirusScan puede examinar o excluir durante una sesión de exploración
- Limitar el número de tareas de exploración que puede crear, configurar y ejecutar desde la Consola de VirusScan

También puede elegir si desea que el servicio de administración de VirusScan se cargue automáticamente al iniciar el equipo.

- **NOTA:** McAfee VirusScan Software recomienda encarecidamente configurar el servicio de administración de VirusScan para que se cargue al iniciar el sistema. De lo contrario, posiblemente no podrá iniciar algunos componentes de VirusScan, y desaprovechará las ventajas de poder compartir datos entre los componentes.

Cómo abrir el panel de control de VirusScan

El funcionamiento del panel de control de VirusScan es muy similar al del panel de control estándar de Windows.

Para abrir el panel de control, siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Configuración** y, a continuación, **Panel de control**.
2. Localice y haga doble clic en el icono del panel de control de VirusScan para abrir el panel de control (consulte la Figura 8-1).

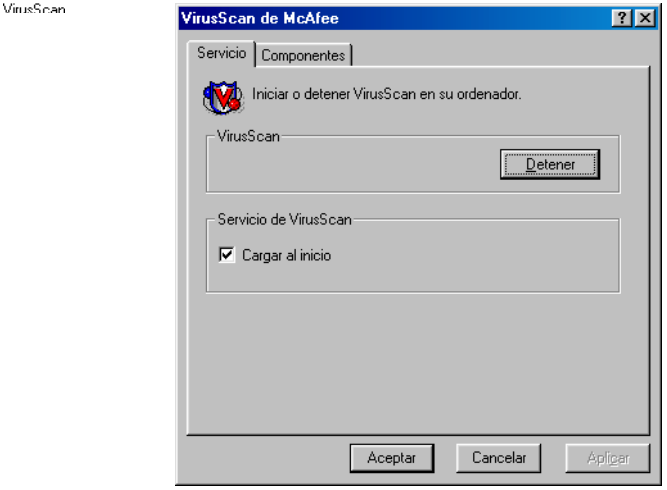

Figura 8-1. Panel de control de VirusScan: página Servicio

Selección de opciones del panel de control de VirusScan

El panel de control consta de dos páginas de propiedades con fichas que muestran las opciones.

Para seleccionar las opciones, siga estos pasos:

1. Abra el panel de control y haga clic en la ficha Servicio.
2. Para detener todos los componentes de VirusScan activos, haga clic en **Detener**.

   Si todos los componentes de VirusScan que se cargan en la memoria, normalmente la Consola y el explorador VShield, están inactivos, este botón indicará **Iniciar**. Haga clic en él para volver a cargar los componentes de VirusScan inactivos.

   También puede reiniciar individualmente la aplicación VirusScan y la Consola desde el menú **Inicio** de Windows.
3. Active la casilla de verificación **Cargar al inicio** en el área de Servicio de VirusScan para iniciar el servicio de administración de VirusScan (AVSYNMGR.EXE) tan pronto como encienda el equipo.

   El servicio de administración supervisa todas las comunicaciones entre los componentes del programa de VirusScan, determina qué componentes debe cargar para realizar tareas del programa y permite iniciar o detener todos los componentes del programa a la vez.

   Si su equipo utiliza Windows NT Workstation versión 4.0 o Windows 2000 Professional, este servicio aparece en el cuadro de diálogo Servicios como AvSync Manager. Si utiliza Windows 95 o Windows 98, no es posible el acceso directo a este servicio.

- **NOTA:** McAfee VirusScan recomienda encarecidamente configurar el servicio de administración de VirusScan para que se cargue al iniciar el sistema. De lo contrario, posiblemente no podrá iniciar algunos componentes de VirusScan, y desaprovechará las ventajas de poder compartir datos entre los componentes.

4. Haga clic en la ficha Componentes para continuar (Figura 8-2).

Figura 8-2. Panel de control de VirusScan: página Componentes

5. Para que el explorador VShield se cargue al encender el equipo, active la casilla de verificación **Cargar VShield al inicio**. Esta misma configuración aparece en la página Detección del módulo Exploración de sistema. Cualquiera de estas configuraciones cargará el explorador al iniciar el equipo.

- **NOTA**: McAfee VirusScan Software recomienda que deje esta casilla activada. El explorador VShield es la mejor defensa constante contra infecciones de virus.

---

6. Haga clic en o introduzca un número en el cuadro de texto de elementos de exclusión para especificar cuántos elementos pueden aparecer en la lista de exclusión del módulo Exploración de sistema de VShield. Esta configuración también determina cuántos elementos pueden aparecer en la lista de exclusión para cualquier tarea de exploración de la aplicación VirusScan o cualquier tarea de exploración que configure desde la Consola de VirusScan.

   De manera predeterminada, pueden aparecer 100 elementos en la lista. El valor que defina aquí no puede ser menor de cinco elementos.

7. Haga clic en o introduzca un número en el cuadro de texto de elementos de exploración para especificar cuántos objetivos puede examinar a la vez la aplicación VirusScan.

Esta configuración define el número máximo de elementos que pueden aparecer como objetivos para cualquier tarea de exploración predeterminada o cualquier tarea que configure desde la Consola de VirusScan. De manera predeterminada, pueden aparecer 100 elementos en la lista. Si añade más de 100 elementos únicos a la lista de exclusión, la aplicación VirusScan puede afectar al rendimiento del sistema. El valor que defina aquí no puede ser menor de cinco elementos.

8. Active la casilla de verificación **Cargar al inicio** en el área de la Consola para que la Consola de VirusScan se inicie tan pronto como encienda el equipo.

   Para poder ejecutar las tareas que tenga programadas, incluidas las de exploración, AutoUpgrade y AutoUpdate, la Consola debe estar en funcionamiento. No obstante, no es necesario iniciar la Consola para poder iniciar el explorador VShield.

9. Haga clic en  o introduzca un número en el cuadro de texto de número máximo de tareas para indicar cuántas tareas de exploración pueden aparecer en la ventana de la Consola de VirusScan.

   De manera predeterminada, pueden aparecer 50 elementos en la lista. Si incluye más de 50 elementos, la ejecución de las tareas puede afectar al rendimiento del sistema. El valor que defina aquí no puede ser menor de cinco elementos.

10. Haga clic en **Aplicar** para guardar los cambios que realice en esta configuración sin cerrar el panel de control. Haga clic en **Aceptar** para guardar los cambios y cerrar el panel de control. Haga clic en **Cancelar** para cerrar el panel de control sin guardar los cambios.

- **NOTA:** Para poder aplicar los cambios que se realicen, el servicio de administración de VirusScan debe reiniciarse a sí mismo y reiniciar todos los componentes de VirusScan activos.

Utilización de la utilidad de configuración de cliente del Administrador de alertas

Todo el software antivirus de McAfee VirusScan incluye una serie de métodos para alertar cuando ha detectado un virus u otro software perjudicial. Entre éstos se incluyen:

- advertencias gráficas y a toda pantalla que aparecen en el equipo local, a menudo con opciones de respuesta
- sonidos del sistema y mensajes personalizados que puede redactar
- mensajes de correo electrónico enviados como respuestas a quienes enviaron elementos infectados, o como advertencias a otros usuarios informándoles de que ha recibido un elemento infectado
- archivos de registro que registran las acciones de los componentes de VirusScan, incluyendo la detección de virus y los sucesos de respuesta
- presentaciones de resúmenes y estadísticas en tiempo real que actualizan sucesos de detección y respuesta

Muchos de estos métodos sólo alertan al usuario si se encuentra junto al equipo observando cómo se ejecuta la operación de exploración. No obstante, si administra una red de estaciones de trabajo que desea dotar de medidas de seguridad, con frecuencia necesitará un método que le informe sobre infecciones cuando se encuentre en una estación de trabajo concreta o incluso cuando no esté conectado a la red. También necesitará un método para recopilar y administrar mensajes de alerta de toda la red en un repositorio central para que pueda responder cuando cualquier estación de trabajo detecte un archivo infectado.

McAfee VirusScan Software proporciona el software del servidor del Administrador de alertas precisamente con ese fin. El software permite centralizar la recopilación y el procesamiento de mensajes de alerta, asignarles prioridades y mensajes personalizados y designar cualquiera de los 11 métodos existentes para distribuir dichos mensajes. Con la serie de productos antivirus versión 5.1, el servidor del Administrador de alertas viene ahora como un paquete independiente junto con el software antivirus VirusScan NetShield de McAfee. Puede instalar este nuevo software del Administrador de alertas con el software de NetShield, o de manera independiente en un equipo que desee utilizar como punto de recopilación de alertas.

Puede instalar varios servidores del Administrador de alertas, tal vez uno para cada dominio o uno en cada equipo de un servidor clúster. Si lo hace, también podrá enviar mensajes de alerta entre servidores del Administrador de alertas y, por consiguiente, a otros equipos de la red o a sistemas de notificación centralizados. Esta función permite a los departamentos MIS (Sistema de información de administración) realizar un seguimiento de las estadísticas sobre virus y las áreas problemáticas.

Para obtener información sobre cómo instalar y configurar la utilidad Administrador de alertas, consulte la *Guía del administrador* de NetShield.

El software de VirusScan como cliente del Administrador de alertas

El software de VirusScan funciona como programa cliente con respecto al software de NetShield y como servidor del Administrador de alertas. Puede enviar "sucesos" de alerta a cualquier servidor del Administrador de alertas que especifique siempre que detecte un virus o software perjudicial. Después, el servidor del Administrador de alertas transmite esos sucesos, y otros que reciba de las demás estaciones de trabajo, como mensajes de alerta mediante los métodos que el usuario o el administrador del sistema haya definido para la distribución de las alertas.

Por otra parte, el software de VirusScan puede enviar los mismos mensajes de alerta como archivos de texto (.ALR) a un directorio de Alertas centralizadas que el servidor del Administrador de alertas puede ver. El servidor del Administrador de alertas comprueba periódicamente si hay nuevos archivos .ALR en el directorio de Alertas centralizadas y si los encuentra distribuye sus mensajes de alerta.

- **NOTA:** McAfee VirusScan Software recomienda enviar los sucesos de alerta directamente a un servidor del Administrador de alertas en vez de hacerlo a través de Alertas centralizadas, a no ser que la configuración de la red no permita utilizar servidores del Administrador de alertas. El servidor del Administrador de alertas puede funcionar junto con el software de Event Orchestrator de McAfee VirusScan para asociar los mensajes de alerta con la aplicación Magic HelpDesk de McAfee VirusScan, para generar listas de problemas y otras funciones.

  Además, los mensajes del Administrador de alertas contienen muchos más datos que los que se envían a través de Alertas centralizadas. Si se activan capturas SNMP al Administrador de alertas, se recopila gran cantidad de información sobre el equipo que genera los mensajes de alerta y la configuración del software.

El cliente de VirusScan puede complementar cualquiera de los dos métodos con alertas DMI (Interfaz de administración de escritorio) para que el software de administración de red, por ejemplo OpenView de Hewlett-Packard, las procese.

Configuración de la utilidad del cliente del Administrador de alertas

El software de VirusScan incluye una sencilla utilidad de configuración de cliente que permite elegir el servidor del Administrador de alertas que desee para recibir sucesos de alerta, designar un directorio de Alertas centralizadas para recibir mensajes de alerta y especificar el valor numérico de los mensajes de alerta DMI que desee enviar.

La configuración de un sistema de alerta completo es un proceso que consta de dos partes: primero, debe activar la utilidad de configuración de cliente del Administrador de alertas y aplicarla al servidor del Administrador de alertas o a la ubicación de Alertas centralizadas correspondiente. A continuación, debe comprobar que ha activado la casilla de verificación **Notificar al Administrador de alertas** en la página de propiedades Alerta de VirusScan en modo avanzado, en la página Alerta de la extensión Exploración del correo electrónico y en las páginas de alerta de cada módulo de VShield que haya activado.

Así se indica a cada componente de VirusScan que envíe un suceso de alerta a la utilidad de cliente del Administrador de alertas cada vez que detecte un virus o un objeto perjudicial. La utilidad de cliente, a su vez, pasa el mensaje de alerta al servidor del Administrador de alertas que designe. Si no configura primero el software para que genere mensajes de alerta, la utilidad cliente no tendrá ningún mensaje que transmitir al servidor del Administrador de alertas para que lo distribuya.

Para iniciar y configurar la utilidad Administrador de alertas, siga estos pasos:

1. Haga clic en **Inicio** en la barra de tareas de Windows, seleccione **Programas** y, a continuación, **McAfee**. Seguidamente, seleccione **Configuración de alertas de VirusScan**.

   Aparece la página Configuración cliente del Administrador de alertas (Figura 8-3 en la página 279).

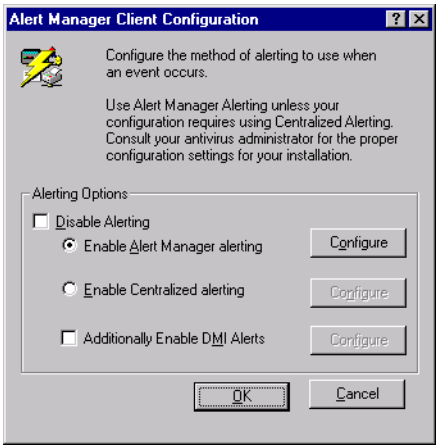

Figura 8-3. Cuadro de diálogo Configuración de cliente del Administrador de alertas

2. Compruebe que la casilla de verificación **Desactivar las alertas** está desactivada. De este modo, se activarán las demás opciones del cuadro de diálogo.

   Active esta casilla sólo si desea que la utilidad de configuración de cliente del Administrador de alertas *no* transmita mensajes de alerta del software antivirus al servidor del Administrador de alertas o al software administrativo DMI (Interfaz de administración del equipo). De manera predeterminada, esta casilla está desactivada. McAfee VirusScan recomienda dejarla desactivada para que el cliente pueda enviar mensajes de alerta. Seleccione el método de alerta que desee utilizar. Podrá elegir entre las siguientes opciones:

   - **Activar alerta del Administrador de alertas**. Haga clic en este botón para enviar sucesos de alerta a un servidor del Administrador de alertas existente en algún punto de la red. Si selecciona esta opción no podrá enviar sucesos de alerta a un directorio de Alertas centralizadas.

     Para seleccionar el servidor de destino, haga clic en **Configurar** para abrir el cuadro de diálogo Seleccionar el servidor del Administrador de alertas (Figura 8-4 en la página 280).

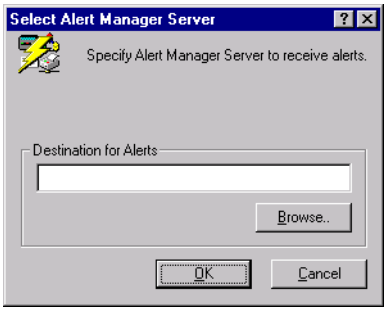

Figura 8-4. Cuadro de diálogo Seleccionar servidor del Administrador de alertas

A continuación, introduzca la ruta de acceso al directorio que contiene el servidor del Administrador de alertas que desee utilizar o haga clic en **Examinar** para localizar el servidor en la red.

Podrá utilizar la notación UNC (Convención de nomenclatura universal) en el cuadro de texto para designar el equipo que contiene el servidor del Administrador de alertas o simplemente escribir su nombre. La utilidad de configuración de cliente del Administrador de alertas validará la forma del nombre que introduzca aquí, pero no comprobará si el servidor del Administrador de alertas existe en el equipo de destino. De este modo, los usuarios de equipos portátiles y otros usuarios remotos pueden designar un servidor del Administrador de alertas aunque no estén conectados a la red.

Si tiene instalados servicios de Directorio activo en el equipo, al hacer clic en Examinar aparece una lista de nombres lógicos del servidor del Administrador de alertas. Si no tiene instalado Directorio activo, sólo se mostrará el árbol del directorio completo. En tal caso, pregunte al administrador del sistema qué equipo contiene el servidor del Administrador de alertas que desea utilizar.

De manera predeterminada, la utilidad cliente utilizará la búsqueda de Directorio activo para localizar un servidor del Administrador de alertas publicado, si tiene instalados los servicios de Directorio activo en este equipo y están funcionando en la red. Para evitar que la utilidad de cliente proceda de este modo, active la casilla de verificación **Desactivar la consulta del directorio activo** cuando aparezca.

Cuando haya seleccionado un destino para los mensajes de alerta, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

- **Activar alertas centralizadas**. Haga clic en este botón para que los componentes de VirusScan envíen mensajes de alerta a un directorio de Alertas centralizadas situado en algún punto de la red. Si selecciona esta opción podrá evitar el envío de sucesos de alerta a un servidor del Administrador de alertas.

  Para seleccionar un directorio de destino, haga clic en **Configurar** para abrir el cuadro de diálogo Configuración de alertas centralizadas (Figura 8-5).

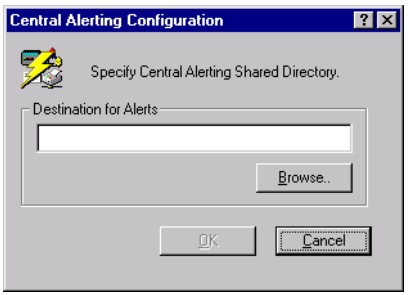

Figura 8-5. Cuadro de diálogo Configuración de alertas centralizadas

A continuación, introduzca la ruta de acceso al directorio de Alertas centralizadas o haga clic en **Examinar** para localizar el directorio en la red. Cuando haya elegido un destino, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

Puede designar cualquier directorio de la red como destino de los mensajes de Alertas centralizadas, pero el directorio debe contener una copia del archivo CENTALRT.TXT para que un servidor del Administrador de alertas pueda transmitir los mensajes de alerta que haya enviado allí.

Si activa Alertas centralizadas, el software de VirusScan envía los mensajes de alerta como archivos de texto con la extensión .ALR al directorio de destino.

Después, podrá seleccionar un servidor designado del Administrador de alertas para el directorio si éste contiene el archivo CENTALRT.TXT, para que compruebe periódicamente si hay archivos .ALR. Si encuentra alguno, extrae del archivo el contenido del mensaje de alerta, distribuye el mensaje mediante uno de sus métodos de notificación preconfigurados y elimina el archivo .ALR. Después aumenta la frecuencia de comprobación del directorio de Alertas centralizadas para capturar otros mensajes que puedan llegar.

- **Añadir activación de alertas**. Active esta casilla de verificación para complementar cualquiera de los otros métodos de alerta. A continuación, haga clic en **Configurar** para abrir el cuadro de diálogo Configuración DMI, donde puede introducir el número de identificación que la aplicación cliente DMI (Interfaz de administración del equipo) asignó al software de VirusScan en el momento de instalarlo (Figura 8-6).

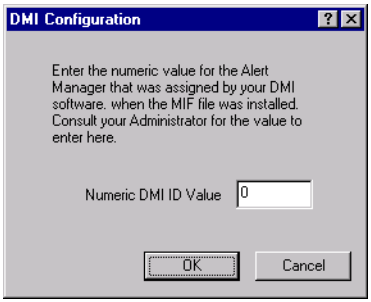

Figura 8-6. Cuadro de diálogo Configuración DMI

Para utilizar esta opción, debe tener una aplicación cliente DMI, por ejemplo OpenView de Hewlett-Packard, instalada en el equipo local y el software administrativo DMI funcionando en algún lugar de la red.

El software de VirusScan incluye un archivo de administración de información (AMG.MIF) que identifica los atributos de alerta de VirusScan para la aplicación cliente DMI. El cliente DMI, a su vez, asigna un número de identificación al software de VirusScan, para que pueda recopilar sucesos de alerta de VirusScan y enviarlos a una aplicación administrativa DMI.

Para que el software de VirusScan pueda enviar los mensajes de alerta con un número de identificación que la aplicación administrativa pueda reconocer y procesar, deberá especificar aquí el número de identificación correcto. Consulte al administrador del sistema para obtener información específica del software DMI.

Cuando haya especificado un número, haga clic en **Aceptar** para cerrar el cuadro de diálogo.

3. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo Configuración de cliente del Administrador de alertas.

Acerca de Safe & Sound 9

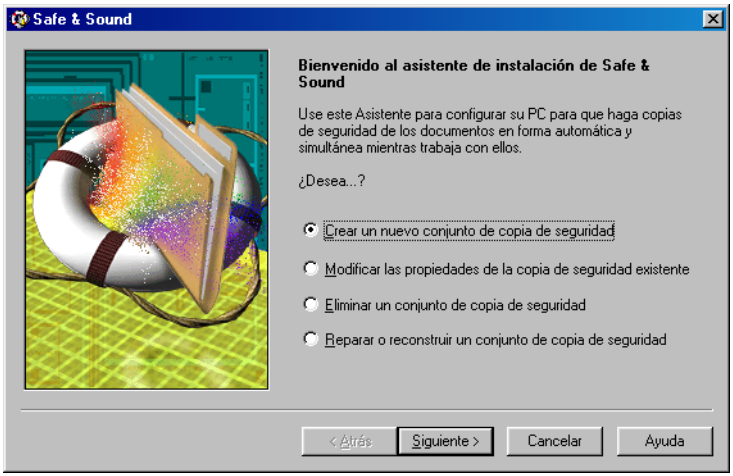

Figura 9-1. Ventana Safe & Sound

El activo más importante del ordenador es la información o *datos*, que el usuario crea y guarda en él. Con el tiempo, el tamaño y valor de estos datos aumenta considerablemente. Los dispositivos de almacenamiento en los que se conserva esta información son vulnerables a una amplia gama de factores humanos y medioambientales que pueden deteriorar o destruir los datos total o parcialmente.

Los datos sobre la estructura de organización del disco, información muy valiosa y vulnerable, también se guardan en distintos lugares de la unidad de disco duro. Esto incluye el sector de arranque, las tablas de particiones, directorios, la FAT (tabla de asignación de archivos) y otros componentes estructurales que Windows utiliza para localizar los datos en la unidad, organizarlos, etc. Si cualquiera de estos componentes se destruye o sufre daños, no podrá acceder a los datos guardados en la unidad.

La FAT, el esquema de la unidad, apunta a las ubicaciones de la unidad en las que están guardados físicamente los archivos. Los archivos pueden guardarse en ubicaciones contiguas o distribuirse en fragmentos en distintas ubicaciones. Puesto que los archivos no siempre se guardan de forma contigua, la información de la FAT es incluso más indispensable que si los archivos se almacenasen uno tras otro. Si la tabla de asignación de archivos de la unidad se deteriora o se mezclan sus datos (efectos que puede causar un virus), el ordenador no podrá localizar ni montar los fragmentos de los archivos. Esto es así aunque los datos de los archivos aún existan.

Utilización de Safe & Sound

Archivo de volumen protegido (la protección de copia de seguridad definitiva)

Con Safe & Sound puede crear juegos de copias de seguridad en archivos de volumen protegido, que es el tipo mejor y más seguro de copia de seguridad. Un *archivo de volumen protegido* es un área independiente de la unidad, denominada algunas veces unidad lógica. Gracias a las características tan especiales de los archivos de volumen protegido de Safe & Sound, este componente puede reconstruir los archivos de copia de seguridad sector por sector, aunque la FAT estándar de la unidad esté deteriorada o se haya perdido por completo. De hecho, los archivos pueden reconstruirse casi por completo aunque se hayan borrado secciones grandes de la unidad o no se puedan leer.

El archivo de volumen protegido incluye también información suficiente en cada entrada de directorio para reconstruir por completo todo el árbol de directorios del archivo aunque se hayan borrado todos sus nodos principales.

Safe & Sound ofrece redundancia interna en las copias de seguridad en archivo de volumen protegido marcando cada sector de cada archivo de la copia de seguridad con información de identificación sobre el contenido del sector y el archivo al que pertenece. Así pues, cada sector de un archivo de volumen protegido contiene información suficiente para que los archivos se reconstruyan a partir de sus sectores individuales.

Razones para realizar copias de seguridad periódicas con Safe & Sound

Los datos son muy valiosos y cuesta mucho recrearlos. Por lo tanto, realizar copias de seguridad frecuentes o incluso duplicadas de los datos importantes de las unidades es *fundamental*. Una copia de seguridad *duplicada* es siempre idéntica a la información de la unidad original.

Safe & Sound automatiza el proceso de copia de seguridad y realiza todas las tareas tediosas y repetitivas. Asimismo, le permite decidir los tipos de archivo que va a incluir en la copia de seguridad, la frecuencia con la que los va a guardar y la ubicación de la copia de seguridad (en la misma unidad, en otra unidad local o en una unidad de red compartida). Con Safe & Sound puede crear juegos de copia de seguridad duplicados que, en un momento dado, son una réplica exacta de los archivos seleccionados para la copia de seguridad en la unidad de origen. También puede especificar una breve demora en la copia de seguridad o realizarla manualmente copiando archivos al juego de copia de seguridad en la unidad, si así lo prefiere.

Todas las formas de almacenamiento de datos pueden perder la información que contienen. Los tipos más frecuentes de almacenamiento de datos: unidades de disco duro, disquetes de 3,5 pulgadas, discos ZIP o cintas SyQuest, se denominan a menudo *almacenamiento permanente* (para diferenciarlos del almacenamiento volátil en la RAM, memoria de acceso aleatorio, del ordenador). Almacenamiento permanente significa que la información permanece intacta aunque se apague el ordenador. Esta modalidad, sin embargo, no significa almacenamiento *eterno*.

Hay muchos factores que pueden causar la pérdida o deterioro de los datos de los disquetes, cintas o unidades: mal funcionamiento del hardware, medios muy usados, tormentas eléctricas, calor excesivo, electricidad estática, imanes, conexiones sueltas de cables o del cable de alimentación, etc. Los discos CD, aunque duraderos, pueden rayarse lo suficiente como para deteriorar los datos que contienen. La intervención del usuario también puede provocar pérdida de datos como, por ejemplo, al borrar la carpeta errónea o dar formato a la unidad que no es. Incluso las aplicaciones bien diseñadas pueden en algunas ocasiones corromper sus propios archivos.

Cuando hay tanto en juego, las copias de seguridad automáticas de Safe & Sound sólo le aportan ventajas. Lo único que tiene que hacer es decidir cuál es la información importante, cómo quiere que se realice la copia de seguridad y dónde se va a guardar. Safe & Sound se encarga de todo lo demás.

Realización de copias de seguridad automáticas con Safe & Sound

Si decide que Safe & Sound cree automáticamente un juego de copia de seguridad, este componente creará el primer juego mientras usted recorre los pasos del asistente de Safe & Sound. A partir de ese momento y mientras esté seleccionada la opción de activación de copias automáticas, seguirá actualizando el juego de copias de seguridad a los intervalos especificados. Si opta por crear copias de seguridad duplicadas, Safe & Sound actualiza el juego de copias de seguridad en el momento en que se guardan de nuevo los archivos fuente originales.

Si selecciona un intervalo de escritura en segundo plano superior a los cero segundos (copia de seguridad duplicada), Safe & Sound actualizará el juego de copia de seguridad en cualquier momento tras el intervalo especificado, durante un periodo de inactividad del PC. De esta forma, Safe & Sound funciona en segundo plano sin interrumpir las tareas que esté realizando el usuario. Se trata de una buena opción para usar con la copia de seguridad en archivo de volumen protegido ya que elimina el problema de reducción de velocidad que provoca el mayor número de accesos al disco y el mayor tamaño de los archivos asociados con este tipo de copia de seguridad.

Definición de la estrategia de copia de seguridad

Una vez decidido el tipo de copia de seguridad que desea utilizar, archivo de volumen protegido o copia de seguridad de directorio, hay una serie de preguntas importantes que debe responder a la hora de definir su estrategia de copia de seguridad:

- ¿Dónde se guardará la copia de seguridad?
- ¿Qué archivos son importantes y por lo tanto deben incluirse en la copia de seguridad?
- ¿Con qué frecuencia debe realizar Safe & Sound estas copias de seguridad?

¿Dónde se guardará la copia de seguridad?

Si el futuro de su empresa depende de que su PC funcione perfectamente en todo momento y si el presupuesto no es un problema, la forma definitiva de proteger los datos del PC es configurar un PC redundante con unidades de tamaño idéntico. La única función de este PC de copia de seguridad sería duplicar los datos del PC principal. Se mantendría a la espera por si el PC principal fallara y, si se diera el caso, lo único que tendría que hacer el usuario sería trabajar en el segundo PC mientras se reparase el principal.

Sin embargo, el dinero suele tener un papel clave a la hora de decidir dónde se van a guardar los juegos de copia de seguridad. Tradicionalmente, la forma más económica de realizar copias de seguridad es copiar los datos en disquetes de 3,5 pulgadas, aunque se trata del método que requiere más trabajo porque hay que cambiar de disquetes manualmente.

En el mercado informático actual, casi es tan económico adquirir una unidad de disco duro independiente para copias de seguridad en la que pueda guardar una copia de seguridad duplicada actual de una o más de las unidades que utiliza en su PC.

Además, podría interesarle guardar la copia de seguridad en una ubicación remota para una mayor protección. Mientras Safe & Sound tenga acceso a una unidad lógica asignada en el PC, podrá guardar allí el juego de copia de seguridad. Es decir, la copia de seguridad puede guardarse en una unidad de red compartida.

- **NOTA:** Puede utilizar el comando Conectar a unidad de red, al que puede acceder haciendo clic con el botón derecho del ratón en Mi PC, para asignar una letra de unidad a una ubicación de la unidad de red. De esta forma, esa ubicación se convierte en una "unidad lógica" del PC. Para obtener más datos, consulte la ayuda en línea de Windows.

Si no puede invertir en otra unidad ni en disquetes para guardar las copias de seguridad, aún puede crear una copia de seguridad de los datos en la misma unidad. En caso de que falle la unidad, la protección que ofrece este método es la mínima, pero las posibilidades de recuperar los datos aumentan al tener dos juegos de la información más importante guardados allí. Las posibilidades aumentan aún más si selecciona el tipo de copia de seguridad en archivo de volumen protegido que permite la recuperación en muchas circunstancias, incluso con la unidad físicamente deteriorada.

- **NOTA:** Si los datos residen normalmente en un servidor, puede hacer una copia local para acceder a los datos incluso cuando el servidor deje de funcionar por cualquier causa.

¿Cuáles son los archivos importantes?

Safe & Sound selecciona automáticamente los archivos que suelen ser importantes para incluirlos en el juego de copia de seguridad. No obstante, puede seleccionar otros archivos o tipos de archivos para incluirlos en la copia de seguridad.

Además, puede crear varios juegos de copia de seguridad para fines concretos. Cada uno de ellos puede crearse cuando y donde especifique el usuario e incluir los archivos o tipos de archivos que se seleccionen. Por ejemplo, podría crear juegos de copia de seguridad individuales para cada uno de sus clientes si genera datos que se guardan en el ordenador como, por ejemplo, diseños publicitarios, imágenes gráficas, libros o datos de contabilidad.

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

Cuanto más reciente sea el juego de copia de seguridad, más seguro se sentirá si el PC tiene algún problema que ponga en peligro la integridad de los datos de las unidades principales. No obstante, es posible que desee conservar el intervalo predeterminado de escritura en segundo plano de 20 minutos para contar con tiempo suficiente para recuperar una versión previa de un archivo si alguna vez lo necesita.

I **SUGERENCIA:** Guarde pronto, guarde con frecuencia. Mientras trabaja, siempre puede pulsar **CTRL-S** para guardar su trabajo sobre la marcha. Cuanto mayor sea la frecuencia con la que guarda, menos perderá en un momento determinado. Otra opción es seleccionar la opción de guardar automáticamente en las aplicaciones para realizar copias de seguridad más frecuentes.

NOTA: Para obtener instrucciones detalladas y más información sobre la utilización de Safe & Sound, consulte el archivo de ayuda en línea de McAfee VirusScan.

Acerca de Cuarentena 10

Utilización del componente de Cuarentena

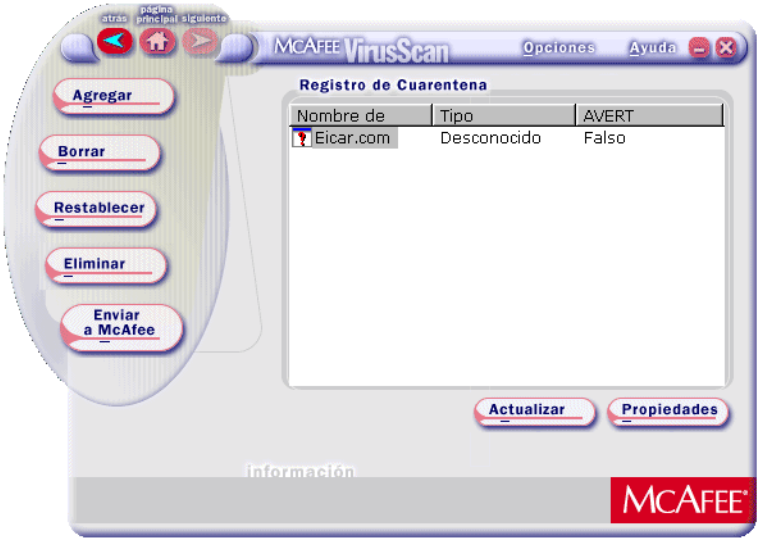

Figura 10-1. Ventana Cuarentena

Con muchos de los componentes de VirusScan puede desplazar los archivos infectados a una carpeta de cuarentena. De esta forma, los retira de las zonas en las que pueden abrirse y puede limpiarlos o borrarlos a su conveniencia.

Para utilizar este componente con archivos infectado que se hayan puesto en cuarentena, siga estos pasos:

1. Inicie la Consola de VirusScan.
2. Haga clic en Cuarentena. Aparece la ventana del explorador de cuarentena.
3. Seleccione un archivo infectado y elija entre las siguientes opciones.
    - Agregar. Seleccione esta opción para poner en cuarentena un archivo bajo sospecha de contener virus.
    - Limpiar. Seleccione esta opción para eliminar el código del virus del archivo infectado. Si no se puede eliminar, la aplicación se lo comunicará en su área de mensajes.

- Restablecer. Seleccione esta opción para colocar de nuevo el archivo en su carpeta original. Esta opción no limpia el archivo por lo que debe asegurarse de que el archivo no está infectado antes de utilizarla.
- Eliminar. Seleccione esta opción para borrar el archivo infectado. Anote la ubicación del archivo para disponer de un registro de archivos borrados. Tendrá que recuperar los archivos eliminados de las copias de seguridad.
- Enviar a McAfee. Seleccione esta opción para enviar nuevos virus a McAfee.

Informes sobre nuevos virus u objetos

McAfee tiene el compromiso de proporcionarle herramientas eficaces y actualizadas que pueda utilizar para proteger su sistema. Con este fin, le pedimos que nos mantenga informados sobre los virus, clases de Java, controles ActiveX o sitios web peligrosos nuevos que VirusScan no pueda detectar en este momento. Recuerde que McAfee se reserva el derecho a utilizar cualquier información que envíe de la manera que considere más adecuada, sin por ello incurrir en obligación alguna.

Si descubre lo que podría ser un virus nuevo o sin identificar, envíe el archivo infectado al equipo de respuesta de emergencia antivirus de McAfee para su análisis, mediante el asistente para envío a McAfee. Puede eliminar sus datos personales del archivo antes de enviarlo.

Envío de información sobre virus al equipo de respuesta de emergencia antivirus

Si descubre lo que podría ser un virus nuevo o sin identificar, envíe el archivo infectado al equipo de respuesta de emergencia antivirus de McAfee para su análisis, mediante el asistente para envío a McAfee. Tenga en cuenta que Network Associates se reserva el derecho a utilizar cualquier información que aporte en la forma en que crea apropiado sin contraer ninguna obligación por ello.

1. Haga clic en Inicio en la esquina inferior izquierda de la pantalla.
2. Seleccione Programas ® McAfee VirusScan ® McAfee VirusScan Central. Se abre VirusScan Central.
3. Haga clic en Cuarentena. Se abre el explorador de cuarentena.
4. Seleccione un archivo de la lista o haga clic en Agregar para añadir un archivo infectado a la lista.

5. Haga clic en Enviar a McAfee. Aparece el asistente McAfee Labs A.V.E.R.T.
6. Haga clic en Siguiente. Aparece una página en la que puede escribir un mensaje para el equipo A.V.E.R.T. Si lo desea, incluya su información personal de contacto. Estos datos son útiles, pero no obligatorios.
7. Haga clic en Siguiente. Aparece una lista de envío.
8. Haga clic en Agregar para seleccionar el archivo o archivos que desea enviar.
    - Otra alternativa es arrastrar y soltar un archivo de Mi PC o Explorador de Windows al cuadro de lista.
    - Para eliminar un archivo de la lista, selecciónelo y haga clic en Eliminar.
9. Haga clic en Siguiente. Aparecerá la página Elegir opciones de carga.
10. Seleccione Suprimir datos del archivo si desea mantener la confidencialidad de sus datos.
11. Si no reside en los Estados Unidos, sustituya la dirección de correo electrónica predeterminada de Network Associates por la dirección local correspondiente.
12. Haga clic en Siguiente. Aparece la página de subsistema de correo electrónico.
    - Si la configuración del sistema así lo requiere, seleccione SMTP y escriba el nombre del servidor SMTP.
    - Seleccione Enviar correo por MAPI si utiliza un servidor de correo compatible con MAPI, por ejemplo, Microsoft Outlook.
13. Haga clic en Finalizar para enviar el archivo.

Extensiones predeterminadas de archivos comprimidos y vulnerables

A

Agregar extensiones de nombre de archivo para explorar

Debido a que normalmente los virus no pueden infectar archivos con código no ejecutable, lo primero que hace el software de VirusScan es buscar virus sólo en aquellos archivos que podrían resultar infectados. El software utiliza una lista de las extensiones de nombre de archivo para realizar un seguimiento de los archivos vulnerables. Esta lista aparece en el cuadro de diálogo Extensiones de programa y es algo que el usuario puede modificar de acuerdo con sus necesidades.

Para cambiar las extensiones que aparecen en el cuadro de diálogo Extensiones de programa, siga los siguientes pasos:

1. Haga clic en **Extensiones** en la página de propiedades Detección para cualquier componente de VirusScan que esté configurando.
2. Aparece el cuadro de diálogo Extensiones de archivos de programa.

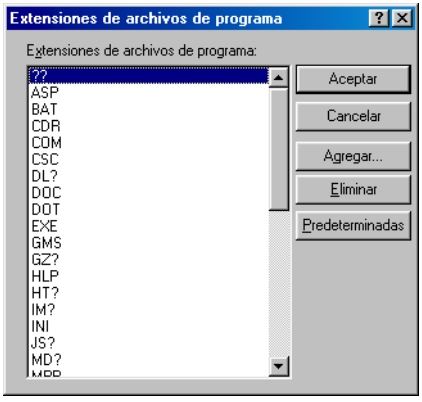

Figura A-1. Cuadro de diálogo Extensiones de archivos de programa

3. Podrá:

   - Hacer clic en **Agregar** para incluir una nueva extensión.

     Esta opción abre el cuadro de diálogo Agregar extensión de archivo de programa. Escriba la extensión de tres caracteres que desee agregar al cuadro de texto que se proporciona. No incluya el punto que suele preceder a la extensión de nombre de archivo. A continuación, haga clic en **Aceptar** para volver al cuadro de diálogo Extensiones de archivos de programa.

     Puede agregar tantas extensiones exclusivas como desee.

   - Seleccionar una de las extensiones que aparecen y, a continuación, hacer clic en **Editar** para cambiar la definición.

   - Seleccionar una de las extensiones que aparecen y, a continuación, hacer clic en **Eliminar** para eliminarla de la lista.

   - Hacer clic en **Predeterminadas** para restaurar las entradas de extensiones originales. Esta opción elimina cualquier extensión que se haya agregado a la lista.

4. Cuando haya finalizado de cambiar la lista, haga clic en Aceptar para guardar los cambios y cerrar el cuadro de diálogo. Haga clic en Cancelar para cerrar el cuadro de diálogo sin guardar los cambios efectuados.

Lista actual de las extensiones de nombres de archivo vulnerables

En esta lista, los símbolos ? son comodines; el software de VirusScan sustituye cualquier carácter por ? con el fin de explorar varios tipos de archivo con extensiones parecidas. Por ejemplo, el software utilizará el comodín .XL? para buscar virus en archivos de plantillas (.XLT) y de hojas de cálculo (.XLS) de Microsoft Excel.

- **NOTA:** McAfee VirusScan Software recomienda realizar una exploración completa del sistema durante la primera exploración o de forma periódica sin poner límite a la exploración de estos tipos de archivos. Esto asegura que el sistema se inicie sin virus. A continuación, el usuario puede utilizar esta lista de extensiones para limitar la envergadura de posteriores operaciones de exploración.

Tabla 10-1. Extensiones de nombre de archivo vulnerables

Extensión	Tipo de archivo	Descripción del archivo
<VACÍO>	Cualquiera	Archivos sin extensión.
.??_	Comprimido	Archivos comprimidos de Windows.
.ARC	De macro/ secuencia de comandos	Archivos LH ARC, versión anterior.
.ARJ	De almacena-miento	Archivos de almacenamiento comprimidos .ARJ de Robert Jung.
.ASP	De macro/ secuencia de comandos	Archivos de las páginas Active Server de Microsoft. Estos archivos contienen las secuencias de comandos que se utilizan con Microsoft Internet Information Server.
.BAT	De programa	Archivos de procesamiento por lotes de DOS.
.CAB	Comprimidos	Archivos binarios de Windows que contienen archivos comprimidos de una aplicación, también denominados archivos "contenedor".
.CDR	De macro	Archivo de documentos de Corel Draw. Las últimas versiones de Corel Draw incluyen un lenguaje de secuencia de comandos que puede generar virus de macro.
.CLA	De programa	Archivos de clase de Java (extensión truncada de .CLASS).
.COM	De programa	Archivos de imágenes binarios o de comandos. Estos archivos se ejecutan igual que los programas ejecutables susceptibles de infectarse. Los archivos de sistema de Windows y DOS utilizan con frecuencia esta extensión.
.CSC	Archivo de comandos/ macro	Archivos de secuencia de comandos de Corel. Los archivos de secuencia de comandos pueden incluir virus o generar virus de macro.
.DL?	De programa	Archivo DLL (biblioteca de vínculos dinámicos); archivos de comandos de cuadros de diálogo de C++. Los archivos DLL son archivos de recursos que se encuentran vinculados a archivos de programa ejecutables. Los archivos ejecutables pueden cargar virus almacenados en ellos mismos y ejecutarlos como parte de su código original.

Tabla 10-1. Extensiones de nombre de archivo vulnerables

Extensión	Tipo de archivo	Descripción del archivo
.DOC	De macro	Archivos de documentos de Microsoft Word. Estos archivos pueden contener macros de Word Basic y, por lo tanto, virus de macros.
.DOT	De macro	Archivos de plantillas de documentos de Microsoft Word. Estos archivos pueden contener macros de Word Basic y virus de macros.
.EXE	De programa	Archivos ejecutables. La mayoría del software utiliza esta extensión para identificar archivos que inician su shell de comandos o núcleo de programa.
.GMS	De macro	Archivos para el almacenamiento global de macros de Corel.
.GZ?	Comprimido	Archivos comprimidos GNU Gzip de UNIX.
.HLP	De macro	Archivos de ayuda de Windows. Estos archivos pueden contener Word Basic ejecutable o cualquier otro código de macros.
.HT?	Archivo de comandos/ macro	Lenguaje de marcado de hipertexto y archivos relacionados; archivos de plantillas de hipertexto de Microsoft. Aunque, por nombre, hacen referencia a texto normal, estos archivos pueden contener eficaces funciones de secuencia de comandos que actúan a través del software del visualizador.
.ICE	Comprimido	Archivos ICE comprimidos.
.IM?	De programa	Archivos de imagen para la creación de imágenes de disco.
.INI	De programa	Archivos de inicialización de Windows. Aunque, por lo general, estos archivos se refieren a archivos de texto, los archivos .INI infectados pueden hacer que los clientes de mIRC realicen acciones no deseadas.
.JS?	Archivo de comandos	Archivos de origen de JavaScript. Los archivos de JavaScript pueden contener código de virus que actúa directamente en los visualizadores de Web.
.LZH	Comprimido	Archivos LHARC comprimidos.

Tabla 10-1. Extensiones de nombre de archivo vulnerables

Extensión	Tipo de archivo	Descripción del archivo
.MD?	De macro	Base de datos de Microsoft Access, complementos y archivos relacionados. Estos archivos pueden contener macros de Visual Basic para Aplicaciones que pueden estar infectadas.
.MPP	De macro	Archivos de Microsoft Project Estos archivos pueden contener macros de Visual Basic para Aplicaciones que pueden estar infectadas.
.MPT	De macro	Archivos de plantillas de Microsoft Project Estos archivos pueden contener macros de Visual Basic para Aplicaciones que pueden estar infectadas.
.MSG	De macro	Archivos de mensajes de Microsoft Mail, Exchange y Outlook. Estos archivos pueden contener secuencias de comandos que pueden introducir infecciones por virus.
.MSO	De macro	Archivos de Microsoft Office 2000.
.OCX	De programa	Controles personalizados de vinculación e incrustación de objetos de Microsoft (OLE). Estos archivos son parecidos a los controles ActiveX y pueden funcionar como software dañino.
.OLE	De programa	Archivos de objetos para vinculación e incrustación de objetos de Microsoft. Estos archivos son parecidos a los controles ActiveX. Se trata de archivos que han sido creados en una aplicación con la finalidad de incrustarlos en otra.
.OV?	De programa	Archivos de superposición.
.POT	De macro	Archivos de plantillas de Microsoft PowerPoint Estos archivos pueden contener macros de Visual Basic para Aplicaciones que pueden estar infectadas.
.PP?	De macro	Archivos de presentaciones y de documentos de Microsoft PowerPoint. Estos archivos pueden contener macros de Visual Basic para Aplicaciones que pueden estar infectadas.

Tabla 10-1. Extensiones de nombre de archivo vulnerables

Extensión	Tipo de archivo	Descripción del archivo
.RAR	De almacena-miento	Archivos de almacenamiento RAR comprimidos.
.RTF	De macro	Archivos RTF (formato de texto enriquecido). Este formato sirve como formato de archivos de texto normal para muchos archivos de documentos.
.SCR	De programa	Archivos de protector de pantalla de Windows.
.SHS	De programa	Archivos de comandos de shell de Windows (Scrap Object Files). Estos archivos pueden introducir comandos que pueden comportarse de forma no deseada en el equipo anfitrión.
.SMM	De macro	Archivos de hoja de cálculo de Lotus AmiPro. Estos archivos incluyen funciones de macro.
.SYS	De programa	Archivos de sistema y controladores de dispositivos de Windows o DOS. Normalmente, estos archivos ejecutables se inician con o forman parte del programa de ejecución.
.TAR	De almacena-miento	Archivos de almacenamiento de cintas de UNIX.
.VBS	Archivo de comandos	Archivos de secuencia de comandos de Visual Basic y archivos de VBScript. VBScript es una implementación del lenguaje de programación de Microsoft Visual Basic. Refuerza funciones especiales de varias páginas Web y puede manipular directamente diversas funciones de Microsoft Outlook y otros programas.
.VS?	De macro	Archivos de dibujo y relacionados de Visio. Las últimas versiones de Visio incluyen extensiones de secuencias de comandos susceptibles de infectarse.
.VXD	De programa	Controladores de dispositivos virtuales de Windows. Hay campos ejecutables que normalmente se encuentran en la memoria.
.WBK	De macro	Archivos de copia de seguridad de Microsoft Word.
.WPD	De macro	Archivos de documentos de Corel WordPerfect.

Tabla 10-1. Extensiones de nombre de archivo vulnerables

Extensión	Tipo de archivo	Descripción del archivo
.XL?	De macro	Archivos de Microsoft Excel de hoja de cálculo, complemento, barra de herramientas, gráfico, cuadro de diálogo, copia de seguridad, macro, área de trabajo, módulo de Visual Basic o plantilla. Estos archivos pueden contener macros de Visual Basic para Aplicaciones que pueden estar infectadas.
.XML	Archivo de comandos/ macro	Archivos con lenguaje de marcado extensible. Aunque por su nombre hacen referencia a texto normal, estos archivos pueden contener potentes funciones de secuencia de comandos que actúan a través del software del visualizador.
.ZIP	De almacena-miento	Archivos de almacenamiento comprimidos WinZip y PKZip.

Lista actual de archivos comprimidos explorados

La aplicación VirusScan y el explorador VShield buscan virus dentro de una gama de formatos de archivos comprimidos y de almacenamiento. Cada componente utiliza tecnologías ligeramente diferentes para realizar su cometido y, por lo tanto, trata cada tipo de archivo de una forma distinta.

Por esta razón, un archivo "comprimido" es un archivo único. Las utilidades de compresión, como PKLite, LZEXE y otras, combinan o eliminan datos redundantes de estos archivos para reducir su tamaño. Un archivo de "almacenamiento" es un archivo que actúa como un "envoltorio" o "sobre" que contiene otros archivos dentro de él. Los archivos del envoltorio pueden o no comprimirse. Ejemplos de tales archivos son los archivos WinZip, .TAR y .ARC. La mayoría de los archivos WinZip comprimen otros archivos y los envuelven en uno sólo.

Esta tabla resume cómo trata cada componente de VirusScan los diferentes tipos de archivos:

Tabla 10-1. Tratamiento de la exploración de archivos comprimidos y de almacenamiento

Componente de VirusScan	Archivo de almacenamiento	Archivo comprimido
aplicación VirusScan	• Active la casilla de verificación **Archivos comprimidos**. • Abre los archivos de almacenamiento y realiza una exploración de los archivos que contiene. • Especifique **Todos los archivos** como el objetivo de exploración o agregue la extensión de nombre de archivo del archivo de almacenamiento en el cuadro de diálogo Extensiones de programa para que la aplicación realice una exploración del archivo de almacenamiento a modo de archivo.	• Active la casilla de verificación **Archivos comprimidos**. • Realiza una exploración de los archivos comprimidos si se especifica **Todos los archivos** como el objetivo de exploración o agregue la extensión del archivo comprimido en el cuadro de diálogo Extensiones de programa.
explorador VShield	• El explorador no abrirá el archivo de almacenamiento para realizar una exploración de los archivos que contiene. • Especifique **Todos los archivos** como el objetivo de exploración o agregue la extensión de nombre de archivo del archivo de almacenamiento en el cuadro de diálogo Extensiones de programa para que el explorador examine el archivo de almacenamiento a modo de archivo.	• Active la casilla de verificación **Archivos comprimidos**. • Especifique **Todos los archivos** como el objetivo de exploración o agregue la extensión del archivo comprimido en el cuadro de diálogo Extensiones de programa para que el explorador detecte los virus en el archivo comprimido.

Ambos componentes de VirusScan cuentan con soporte incorporado para varios formatos de archivos comprimidos o de almacenamiento. La tabla que aparece a continuación muestra los formatos y describe la forma en que los explora cada componente al activar la casilla de verificación Archivos comprimidos. Puede que no haya modificado o agregado elementos a esta lista.

Tabla 10-1. Cómo trata el software de VirusScan cada tipo de archivo

Formato	Descripción	Compatibilidad con la aplicación VirusScan	VShield del explorador VShield
.??_	Archivo comprimido de Windows	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa
.GZ?	Archivo comprimido GNU Gzip de UNIX	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa
.TD0	Archivo comprimido Teledisk	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa
.ARC	Archivo LH ARC, versión anterior	• Explora el archivo de almacenamiento • Explora los archivos contenidos en el archivo de almacenamiento	• Explora el archivo de almacenamiento como un archivo normal si aparece en la lista del cuadro de diálogo Extensiones de programa • No examinará los archivos contenidos en el archivo de almacenamiento

Tabla 10-1. Cómo trata el software de VirusScan cada tipo de archivo

Formato	Descripción	Compatibilidad con la aplicación VirusScan	VShield del explorador VShield
.ARJ	Archivo comprimido .ARJ de Robert Jung	• Explora el archivo de almacenamiento • Explora los archivos comprimidos contenidos en el archivo de almacenamiento	• Explora el archivo de almacenamiento como un archivo normal si aparece en la lista del cuadro de diálogo Extensiones de programa • No explorará los archivos comprimidos contenidos en el archivo de almacenamiento
.CAB	Archivo binario de Windows que contiene archivos comprimidos de una aplicación, también denominado archivo "contenedor".	• Explora el archivo de almacenamiento • Explora los archivos comprimidos contenidos en el archivo de almacenamiento	• Explora el archivo de almacenamiento como un archivo normal si aparece en la lista del cuadro de diálogo Extensiones de programa • No explorará los archivos comprimidos contenidos en el archivo de almacenamiento
.ICE	Archivo ICE comprimido	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa
.LZH	Archivo LHARC comprimido	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa	• Explora el archivo comprimido si aparece en la lista del cuadro de diálogo Extensiones de programa

Tabla 10-1. Cómo trata el software de VirusScan cada tipo de archivo

Formato	Descripción	Compatibilidad con la aplicación VirusScan	VShield del explorador VShield
.RAR	Archivo de almacenamiento RAR comprimido	• Explora el archivo de almacenamiento • Explora los archivos contenidos en el archivo de almacenamiento	• Explora el archivo de almacenamiento como un archivo normal si aparece en la lista del cuadro de diálogo Extensiones de programa • No examinará los archivos contenidos en el archivo de almacenamiento
.TAR	Archivo de almacenamiento de cintas de UNIX	• Explora el archivo de almacenamiento • Explora los archivos contenidos en el archivo de almacenamiento	• Explora el archivo de almacenamiento como un archivo normal si aparece en la lista del cuadro de diálogo Extensiones de programa • No examinará los archivos contenidos en el archivo de almacenamiento
.ZIP	Archivo PKZip o WinZip	• Explora el archivo de almacenamiento • Explora los archivos comprimidos contenidos en el archivo de almacenamiento	• Explora el archivo de almacenamiento como un archivo normal si aparece en la lista del cuadro de diálogo Extensiones de programa • No explorará los archivos comprimidos contenidos en el archivo de almacenamiento

Servicios de soporte técnico para el producto B

Actualizaciones

Durante un año, recibirá de forma gratuita actualizaciones de los archivos de firmas de virus. La actualización periódica de estos archivos para McAfee VirusScan es fundamental para garantizar la detección de todos los virus nuevos y la total protección del sistema.

Para actualizar los archivos de firmas, sólo tiene que hacer clic en el botón ACTUALIZAR de la página de inicio de McAfee VirusScan. Compruebe que el PC está conectado a Internet ya que VirusScan actualizará automáticamente los archivos.

Una vez transcurrido el periodo de un año tras la adquisición del software, puede contratar otro año de actualizaciones de archivos de firmas DAT por un precio aproximado de 1.000 pts (4,95 dólares).

Cómo ponerse en contacto con McAfee

ANTES DE PONERSE EN CONTACTO CON McAfee Software para solicitar asistencia técnica, sitúese ante el ordenador que tenga McAfee VirusScan instalado y compruebe la información que se indica a continuación:

- ¿Ha enviado la tarjeta de registro del producto?
- Versión de McAfee VirusScan
- Nombre del cliente, si se ha registrado
- Modelo de disco duro (interno o externo)
- Versión del software del sistema
- Memoria (RAM)
- Monitores, placas o tarjetas adicionales
- Nombre y versión del programa de software que causa problemas
- Mensaje de error EXACTO que aparece en pantalla
- Pasos que se han realizado antes de recibir el mensaje de error
- Una completa descripción del problema

Servicio de atención al cliente

Para realizar pedidos u obtener información sobre productos, póngase en contacto con el Servicio de atención al cliente de McAfee en el número 901 11 67 32 o escriba a la siguiente dirección:

McAfee Software Division
P.O. Box 898
7301 BC Apeldoorn
Paises Bajos

Si necesita asistencia adicional o tiene preguntas concretas sobre nuestros productos, envíe un mensaje de correo electrónico a la dirección adecuada:

- Para preguntas de carácter general sobre pedidos de software: mcafeestore@beyond.com
- Para obtener ayuda sobre la descarga del software: mcafeedownloadhelp@beyond.com
- Para comprobar el estado de un pedido: mcafeeorderstatus@beyond.com
- Para solicitar información sobre una promoción: mcafeepromotions@beyond.com

Soporte técnico

Soporte a través de la web

McAfee es conocido por su dedicación para satisfacer a sus clientes. Hemos continuado esta tradición haciendo de nuestro sitio en la World Wide Web (http://www.mcafeehelp.com) un recurso de gran utilidad donde obtener respuestas a cuestiones de soporte técnico.

Le animamos a que sea ésta su primera fuente a la hora de obtener respuestas a las preguntas más frecuentes, para actualizar el software de McAfee o para tener acceso a las noticias de McAfee y a la información sobre virus.

Aproveche las ventajas del McAfee Product KnowledgeCenter, su centro de soporte en línea gratuito, 24 horas al día, 7 días a la semana (http://www.mcafeehelp.com).

Información para descargas (ID de licencia: VSF500RSP) C

Como cliente de McAfee a quien tenemos en gran estima, nos comprometemos a mantener su sistema LIBRE de virus. Como medida de protección contra las nuevas amenazas de virus, mantenga la instalación de VirusScan actualizada.

De acuerdo con las condiciones de su acuerdo de licencia con McAfee, tiene derecho a una (1) ampliación GRATUITA dentro del periodo de noventa (90) días posterior a la fecha de adquisición. En este documento se explican las distintas formas de acceder a la ampliación GRATUITA de VirusScan.

Si tiene problemas a la hora de descargar o aplicar los archivos de ampliación mediante cualquiera de los métodos que se indican a continuación, puede llamar al Soporte técnico de McAfee al 972-855-7044.

SecureCast™ (para la versión comercial para Windows 95/98):

SecureCast es la forma más sencilla de Actualizar y Ampliar la copia de VirusScan para Windows 95/98. Con un solo clic del ratón, SecureCast incluirá automáticamente en su sistema las actualizaciones del software y la ampliación GRATUITA del producto. Para actualizar la copia de VirusScan, sólo tiene que hacer clic en el botón Actualizar de la interfaz de VirusScan Central.

Acceso a Internet

Necesitará un navegador web (WWW) como, por ejemplo, Internet Explorer, Netscape o el navegador web AOL para acceder al sitio web de McAfee.

1. Escriba la dirección web de la página de inicio de McAfee en el área correspondiente del navegador de Internet. Escriba: http://www.mcafee.com
2. Una vez cargada la página de inicio de McAfee, haga clic en la ficha "descargar".
3. Cuando se abra la página del centro de descarga (http://www.mcafee.com/centers/download/), localice el vínculo "Ampliaciones" resaltado y subrayado, y haga clic en él.

4. En la página de información sobre ampliaciones, haga clic en el vínculo Ampliar antivirus de McAfee.

5. En la página de ampliación de antivirus de McAfee, escriba el ID de licencia:, que se incluye al principio de esta tarjeta, en el sitio que corresponda. Pulse el botón para enviar.

6. En la página de identificación de cliente de antivirus de McAfee, escriba su dirección de correo electrónico en el espacio provisto a tal fin y pulse el botón para enviar.

7. Si ha registrado previamente el producto, aparecerá la página de agradecimiento. Para iniciar la descarga del producto, haga clic en el botón de descarga.

8. Si no ha registrado el producto previamente, aparecerá la página de registro de producto de McAfee. Se le pedirá que indique su apellido, nombre, código postal, país, localidad y una contraseña de su elección. Pulse el botón para enviar. Una vez enviado, aparecerá en pantalla una página de agradecimiento. Automáticamente se le enviará una URL de acceso a la dirección de correo electrónico facilitada.

9. Al abrir el mensaje de correo electrónico, se le indicará que haga clic en la url adjunta. Aparece un mensaje de agradecimiento con un botón de descarga. Haga clic en este botón para iniciar la descarga.

10. Una vez descargado el archivo y guardado en el disco duro, extraiga o descomprima el archivo (si es necesario) y ejecute el programa de instalación.

La información de este documento se proporciona "tal y como es" sin garantía de ningún tipo. En ningún caso, McAfee se hará responsable de los daños en que se incurra por la utilización o uso incorrecto de la información de este documento. Puesto que algunos estados no permiten la exclusión o limitación de responsabilidades por daños directos o indirectos, la limitación anterior puede no ser aplicable en su caso.

Uso del servicio SecureCast para obtener nuevos archivos de datos

D

Introducción al servicio SecureCast

El servicio SecureCast de McAfee VirusScan proporciona un método cómodo para recibir las últimas actualizaciones de archivos (.DAT) de definición de virus de forma automática a medida que estén disponibles y sin tener que descargarlos. El servicio SecureCast utiliza la tecnología BackWeb de "empuje" para enviar nuevos archivos, mensajes de alerta y cualquier otra información mediante el canal Enterprise SecureCast, al que es posible suscribirse al registrarse con McAfee VirusScan.

Para utilizar esta opción, hay que descargar el software de cliente BackWeb que se encuentra disponible en el sitio Web de McAfee:

http://www.nai.com/asp_set/anti_virus/alerts/register.asp

NOTA: Los clientes empresariales deben disponer, en primer lugar, de un número de concesión o número de serie del producto para suscribirse al canal Enterprise SecureCast.

Si no lo tiene, póngase en contacto con el agente de compra, distribuidor o servicio de atención al cliente de McAfee VirusScan en uno de los siguientes números de teléfono para obtener ayuda: 00800-122-55-624 para Alemania, Bélgica, Dinamarca, España, Finlandia, Francia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia y Suiza. 00800-312-21-287 para Grecia. 1-800-552-171 para Irlanda. 0800-995-054 para Sudáfrica. 00800-319-29-147 para Turquía.

Si ya es un cliente registrado de McAfee VirusScan y no conoce su número de concesión, envíe el formulario en línea de solicitud de número de concesión:

http://www.nai.com/asp_set/anti_virus/alerts/grantreq.asp

O bien

Envíe un mensaje de correo electrónico a la dirección adecuada:

entsecast@nai.com (Estados Unidos)

esc_registration_Europe@nai.com (Europa)

esc_registration_asia@nai.com (Asia)

McAfee VirusScan proporciona una amplia sección de las preguntas más frecuentes que pueden contestar a la mayoría de las dudas relacionadas con la configuración y la descarga de SecureCast. Para consultar esta lista de las preguntas más frecuentes, visite el sitio Web de McAfee VirusScan:

http://www.nai.com/asp_set/anti_virus/alerts/faq.asp

¿Por qué se deben actualizar los archivos de datos?

El software cuenta con información en sus archivos de definición de virus (.DAT) para identificar dichos virus. Cada mes aparecen más de 200 nuevos virus; sin embargo, es posible que los antiguos archivos .DAT no los reconozcan. Para hacer frente a este reto, McAfee VirusScan proporciona archivos .DAT nuevos cada semana. El usuario puede utilizar estas actualizaciones de archivos de datos de forma gratuita con su versión del software. Si no utiliza los archivos .DAT actuales, puede poner en peligro la seguridad antivirus. McAfee VirusScan recomienda encarecidamente actualizar los archivos .DAT periódicamente.

IMPORTANTE: La utilización de archivos de identificación de virus actualizados es sólo un elemento de un programa antivirus eficaz. Es igualmente importante utilizar un motor de exploración que incorpore avances actuales en la detección y limpieza de virus. McAfee VirusScan lanza periódicamente nuevas versiones de su motor de exploración que incorporan estos avances.

Sin embargo, los archivos .DAT anteriores puede que no funcionen correctamente con motores de exploración más recientes. Cuando la versión del motor de exploración anterior se vuelva obsoleta, McAfee VirusScan interrumpirá el desarrollo de archivos .DAT para él. Debe obtener una nueva versión del software antes de que la versión actual se quede obsoleta.

¿Qué archivos de datos proporciona el servicio SecureCast?

Con el servicio SecureCast, se descargarán automáticamente los siguientes archivos:

- **Nuevas versiones de productos**. Las nuevas versiones de productos que recibirá mediante SecureCast dependerán de los términos de la licencia o concesión.
- **Actualizaciones de definición de virus**. Semanalmente recibirá actualizaciones de archivos .DAT de la versión del producto.
- **Actualizaciones del paquete SuperDAT**. Los paquetes SuperDAT cuentan con actualizaciones de archivos .DAT (exactamente las mismas actualizaciones que el usuario recibe mediante el paquete semanal) y con nuevas versiones del motor de exploración, conforme se van encontrando disponibles. La utilidad SuperDAT también cuenta con la característica de tener una arquitectura de configuración sencilla para rápidas actualizaciones y nuevas versiones de archivos .DAT y de motores de exploración.
- **Mensajes de alerta de virus**. Los investigadores de AVERT publican mensajes de alerta de virus que informan a los clientes acerca de las amenazas de virus con mucho riesgo. Estos mensajes conectan al cliente directamente con el sitio Web de AVERT, donde es posible descargar archivos EXTRA.DAT, si se encuentran disponibles, para calibrar la amenaza y para informar acerca de las características del nuevo virus.

Instalación del cliente BackWeb y del servicio SecureCast

La instalación del servicio SecureCast y el cliente BackWeb implica un proceso de dos fases:

1. Descargar e instalar el cliente BackWeb
2. Registrarse para recibir los InfoPaks del servicio SecureCast

Para iniciarse en el servicio SecureCast, consulte los requisitos del sistema que aparecen más abajo y, a continuación, siga los pasos que se describen en cada sección.

Requisitos del sistema

El software de cliente BackWeb instalará y se ejecutará en cualquier equipo personal con:

- Un procesador Intel o cualquier procesador compatible
- Windows 95, Windows 98, Windows NT o Windows 2000
- Por lo menos, 10MB de espacio libre en disco, además de espacio suficiente para el producto y otras descargas
- Una conexión activa a Internet, directa o por acceso telefónico, de al menos una hora de duración por semana

Fase 1: Descargar e instalar BackWeb

1. Para descargar el software de cliente BackWeb, hay que conectarse al sitio Web de McAfee:

   http://www.nai.com/asp_set/anti_virus/alerts/register.asp

   A continuación, descargue el archivo ESC_501.EXE en un directorio temporal del disco duro.

   Si el producto está en CD-ROM, seleccione el servicio SecureCast de las opciones de instalación que se proporcionan en el CD-ROM o ubique el archivo ESC_501.EXE en su CD-ROM.

2. Haga doble clic en el icono de programa para empezar.

   Tan pronto como el programa de instalación haya extraído los archivos de instalación necesarios, aparecerá el primer panel de instalación de BackWeb (vea la Figura D-1 en la página 309).

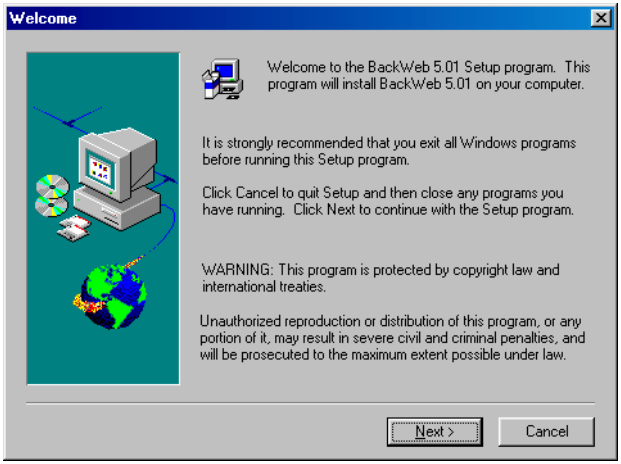

Figura D-1. Panel de bienvenida del cliente BackWeb

3. Lea las instrucciones y las advertencias que aparecen en este panel, a continuación, haga clic en **Siguiente>** para continuar.

4. Aparece el acuerdo de licencia de BackWeb (Figura D-2).

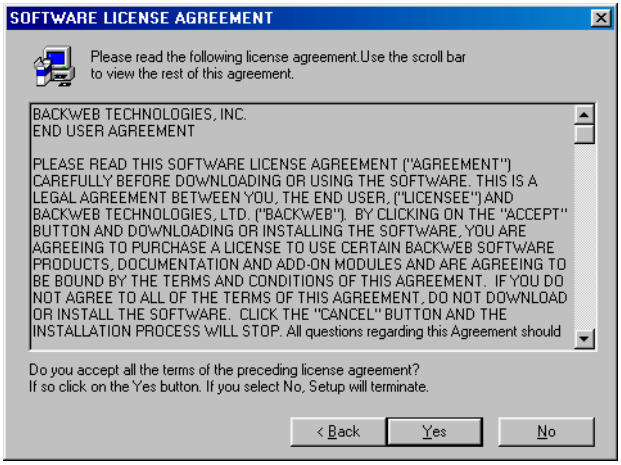

Figura D-2. Panel de acuerdo de licencia del software BackWeb

5. Haga clic en **Sí** para continuar.

6. Aparece el panel Seleccionar ubicación de destino (Figura D-3 en la página 310).

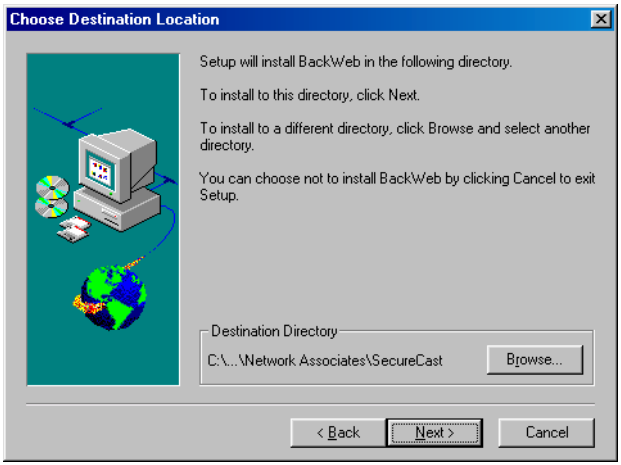

Figura D-3. Panel Seleccionar ubicación de destino

7. Escriba una nueva ubicación para el programa de instalación con el fin de instalar el software cliente, si lo desea, o haga clic en **Examinar** para encontrar una carpeta apropiada. Haga clic en **Siguiente>** para continuar.

   El programa de instalación comenzará a copiar los archivos de programa de BackWeb en el equipo. Mientras se está realizando, se muestra el proceso en la pantalla. Una vez finalizado, el programa de instalación muestra la ventana Tipo de conexión (Figura D-4).

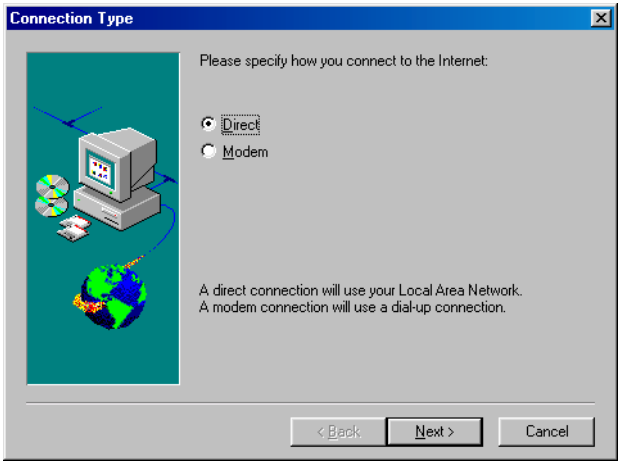

Figura D-4. Panel Tipo de conexión

8. Especifique el tipo de conexión que tiene su equipo con Internet. Podrá elegir entre las siguientes opciones:

   - **Directa**. Seleccione esta opción si se conecta a Internet a través de una red de área local, una conexión con un ancho de banda alto como un módem por cable o una conexión DSL. Continúe con el Paso 9.
   - **Módem**. Seleccione esta opción si tiene que marcar para conectarse a un proveedor de servicios de Internet o en su propia red corporativa. Vaya al Paso 13.

   Aparece el panel Método de comunicación (Figura D-5).

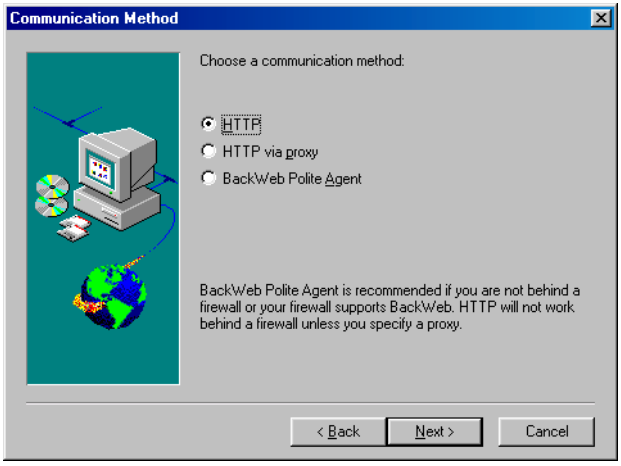

Figura D-5. Panel Método de comunicación

9. Elija un método de comunicación. Podrá elegir entre las siguientes opciones:

   - **HTTP**. Seleccione esta opción si puede conectarse directamente a Internet sin tener que hacerlo a través de un servidor proxy. Vaya al Paso 13.
   - **HTTP mediante proxy**. Seleccione esta opción si se conecta a Internet a través de un servidor proxy en la red. Continúe con el Paso 10.

- **Polite Agent de BackWeb**. Seleccione esta opción para conectarse a Internet a través de una conexión UDP (Universal Datagram Protocol, Protocolo de datagramas universal). Esto permite controlar el comportamiento del cliente BackWeb con respecto a otras aplicaciones que puede que se ejecuten cuando los InfoPaks de SecureCast llegan a su equipo. Para obtener más información, consulte la ayuda en línea de BackWeb en http://www.backweb.com/.

  A continuación, vaya al Paso 13.

10. Si ha seleccionado **HTTP mediante proxy** como método de conexión, aparece el panel Configurar proxy HTTP (Figura D-6).

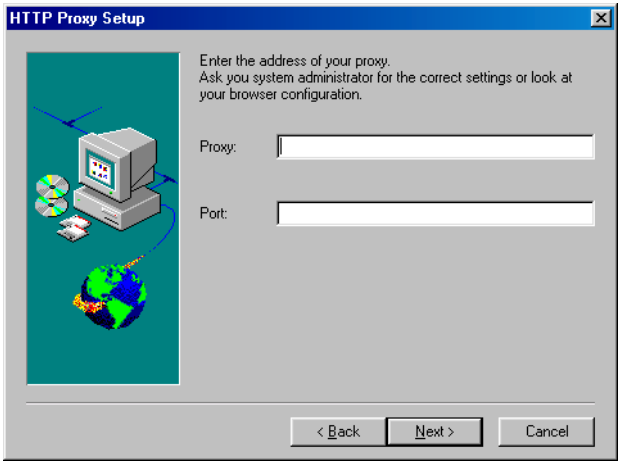

Figura D-6. Panel Configurar proxy HTTP

11. Escriba el nombre del servidor proxy en el cuadro de texto Proxy y, a continuación, escriba el puerto que utiliza el servidor para comunicarse en el cuadro de texto Puerto.

    Cuando termine, haga clic en **Siguiente>** para continuar. Aparece el panel Autenticación de proxy (Figura D-7 en la página 313).

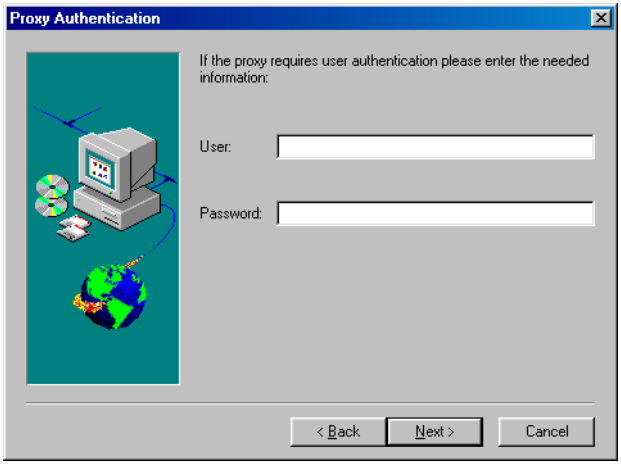

Figura D-7. Panel Autenticación de proxy

12. Si el servidor proxy requiere autenticación de usuario, escriba en los cuadros de texto que se proporcionan un nombre de usuario y una contraseña con suficientes derechos como para permitirle establecer una conexión y, a continuación, haga clic en **Siguiente**> para continuar.

    Aparece el panel Instalación completa (Figura D-8).

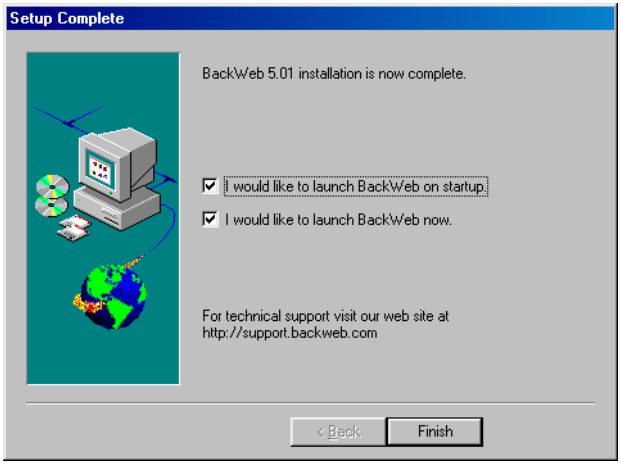

Figura D-8. Panel Instalación completa

13. Para iniciar inmediatamente, deje activadas ambas casillas de verificación en la pantalla y, a continuación, haga clic en **Finalizar** para completar la instalación.

Fase 2: Registrarse con el servicio Enterprise SecureCast

Después de instalar el cliente BackWeb e iniciarlo, el servicio SecureCast abre inmediatamente la aplicación del cliente y envía el primer InfoPak: el formulario de registro de SecureCast (Figura D-9).

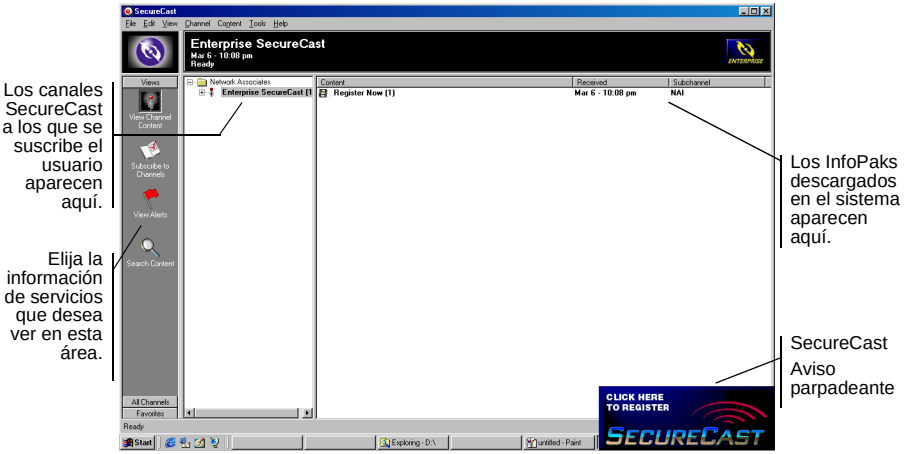

Figura D-9. La ventana de cliente Enterprise SecureCast

El servicio SecureCast le informa de que ha llegado un InfoPak mediante el mensaje parpadeante que aparece en la esquina inferior derecha de la Figura D-9.

IMPORTANTE: Para los usuarios empresariales que tienen una conexión con Internet de alta velocidad, en la ventana puede aparecer **Registrar ahora** como InfoPak ya recibido. Continúe con el Paso 1.

Para los usuarios que tienen una conexión más lenta o que tienen un tráfico anormalmente denso en el sitio del servicio SecureCast o en el suyo, puede que en la ventana no aparezcan InfoPaks. En ese caso, minimice o cierre la ventana BackWeb. Después de un tiempo, recibirá un mensaje parpadeante. Haga clic en el mensaje parpadeante y, a continuación, continúe con el Paso 2.

Para registrarse en el canal Enterprise SecureCast, siga estos pasos:

1. Cuando aparezca en la ventana la opción **Registrar ahora**, haga doble clic en ella. Aparece el aviso parpadeante del servicio SecureCast (Figura D-10).

Figura D-10. Aviso parpadeante de SecureCast

2. Haga clic en el aviso. Aparece el panel de bienvenida de Network Associates (Figura D-11).

Figura D-11. Panel de bienvenida de Network Associates

3. Consulte la información que aparece y, a continuación, haga clic en la opción **Registrar ahora** que aparece en la parte inferior de la pantalla.
4. Haga doble clic en el icono **Registro BW** 

en la ventana que se abre a continuación. Aparece un formulario de información de registro (Figura D-12 en la página 316).

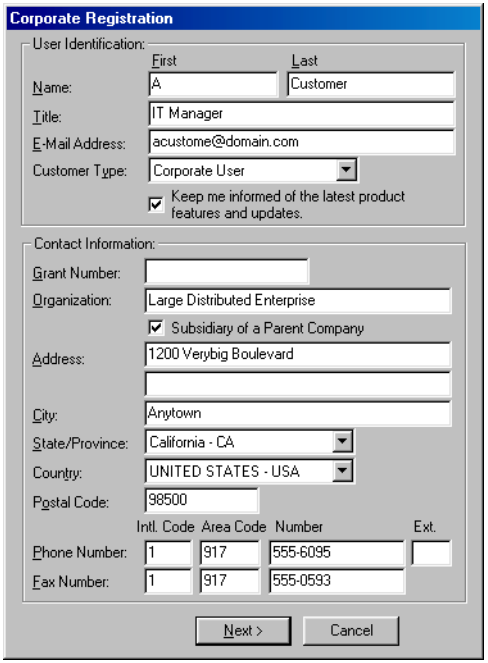

Figura D-12. Formulario de información de registro para usuarios de SecureCast

5. Escriba su nombre, profesión e información de contacto de su empresa en los cuadros que se proporcionan. Tendrá que escribir también el número de concesión recibido al adquirir el software o el que le ha proporcionado el servicio de atención al cliente de McAfee.

NOTA: Si su empresa no es una filial de otra empresa, desactive la casilla de verificación **Filial de empresa matriz** antes de continuar.

Cuando haya escrito la información pertinente, haga clic en **Siguiente>** para continuar.

- Si no ha desactivado la casilla de verificación **Filial de empresa matriz**, aparece el cuadro de diálogo **Información sobre empresa matriz** (vea la Figura D-13 en la página 317). Vaya al Paso 7 en la página 317.
- Si ha desactivado la casilla de verificación **Filial de empresa matriz**, continúe con el Paso 6 en la página 317.

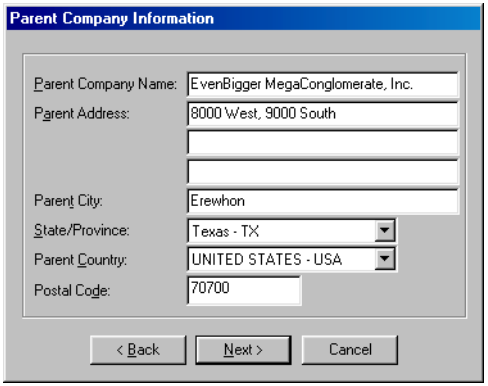

Figura D-13. Formulario de información sobre la empresa matriz de SecureCast

6. Si su empresa es una filial de otra empresa, escriba información de contacto para la empresa matriz en los cuadros de texto que se proporcionan.

   Cuando haya terminado, haga clic en **Siguiente>**. Aparece el cuadro de diálogo **Configuración de comunicación de proxy** (Figura D-14).

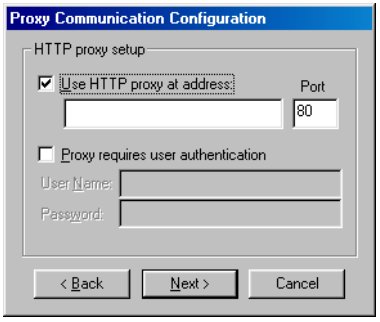

Figura D-14. Configuración de comunicación de proxy de SecureCast

7. Si su red requiere conectarse a Internet a través de un servidor proxy, active la casilla de verificación Utilizar proxy HTTP en la dirección y, a continuación, escriba el nombre de servidor o la dirección IP en el cuadro de texto que se proporciona. A continuación, compruebe que aparece el número de puerto correcto en el cuadro de texto Puerto o escriba el número de puerto correcto.

   Si el servidor proxy requiere que el usuario firme para poder utilizarlo, active la casilla de verificación **Proxy requiere autenticación de los usuarios** y, a continuación, escriba un nombre de usuario y una contraseña con derechos suficientes.

8. Cuando haya terminado, haga clic en **Siguiente>**. Aparece el panel **Estado de actividad en línea** que muestra el progreso del proceso de registro (Figura D-15).

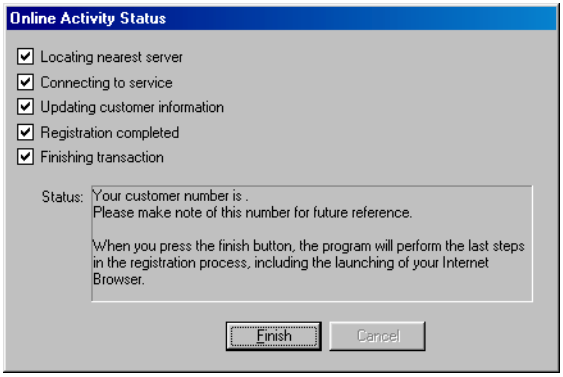

Figura D-15. Panel Estado de actividad en línea de SecureCast

9. Haga clic en **Finalizar** cuando aparezca una marca de verificación en todas las casillas.

   El proceso de instalación ha finalizado. Llegados a este punto, el visualizador de Web se conectará a la página electrónica del servicio de atención al cliente SecureCast de McAfee. Para los usuarios empresariales, el panel será similar al que se muestra en la Figura D-16:

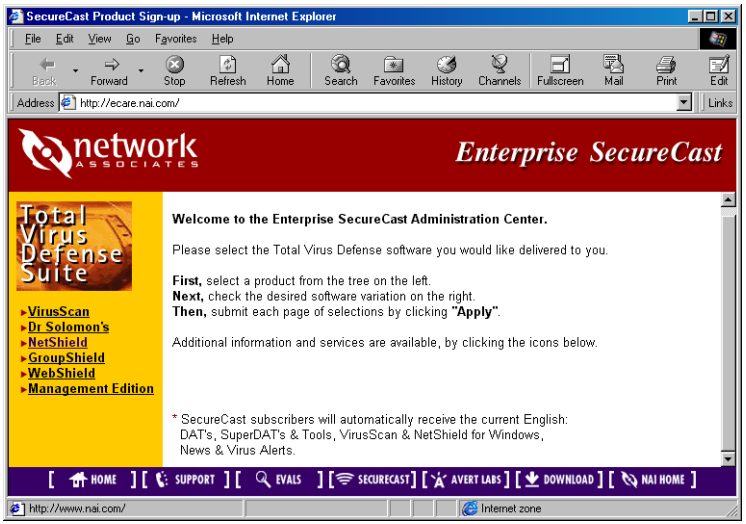

Figura D-16. Servicio electrónico de atención al cliente empresarial SecureCast

Puede utilizar esta página para descargar las actualizaciones y nuevas versiones del producto, ponerse en contacto con el soporte técnico y obtener información directamente de McAfee. Los términos de concesión del usuario determinarán la información que ve aquí y lo que puede descargar.

Solución de problemas del servicio Enterprise SecureCast

Problemas de registro

Si intenta registrarse durante una hora de mucha actividad en la Web, es posible que haya cierta demora cuando el servidor trate de procesar la solicitud de registro. Si recibe el mensaje de error "1105 Error" (error 1105) o "Database Error: Unable to connect to the data source" (error de base de datos: no se puede conectar con el origen de datos), es que existe un problema de base de datos en el servidor. Envíe de nuevo el formulario o intente registrase más tarde. Si sigue teniendo problemas para suscribirse al canal Enterprise SecureCast, póngase en contacto con los servicios de asistencia de descarga de McAfee (lunes a viernes, 8 A.M. a 6 P.M. CET en el siguiente número de teléfono de los Países Bajos: 00 31 20 586 6100.

Cancelación de suscripción de SecureCast

Puede hacer que el servicio SecureCast deje de distribuir InfoPaks cuando lo desee. Para ello, haga clic con el botón derecho del ratón en el icono de BackWeb en la bandeja del sistema Windows y, a continuación, seleccione **Iniciar SecureCast** desde el menú contextual que aparece.

A continuación, siga los siguientes pasos:

1. En el cuadro de lista de la parte izquierda de la ventana de cliente BackWeb (vea la Figura D-9 en la página 314), localice y, a continuación, seleccione el listado del canal SecureCast al que se encuentra suscrito.

2. Haga clic con el botón derecho del ratón en el icono del canal y, a continuación, seleccione **Cancelar suscripción** en el menú contextual que aparece.

   Todos los InfoPaks que aparecen en la lista en la ventana de servicio SecureCast desaparecerán. El servicio SecureCast ya no distribuirá InfoPaks desde ese canal.

Recursos de soporte

Servicio SecureCast

Si tiene más dudas acerca del servicio SecureCast, consulte la sección de preguntas más frecuentes del servicio SecureCast en el sitio Web de McAfee:

http://www.nai.com/asp_set/anti_virus/alerts/faq.asp

Cliente BackWeb

- Para ver una guía completa de BackWeb, incluidas sugerencias adicionales para la resolución de problemas, consulte el Manual del usuario de BackWeb en línea:

  http://www.backweb.com/

Índice

Símbolos

¿por qué preocuparse por los virus?, xiv

"virus" EICAR, usar para comprobar la instalación, 58

A

Activar

en el menú **Tarea**, 203

Active Virus Defense

VirusScan como componente de, 27

Administrador de alertas

utilizar Alertas centralizadas con, 275

alarmas, falsas, identificación, 67

Alertas centralizadas

activar para utilizar con el Administrador de alertas, 275

necesidad del archivo CENTALRT.TXT, 275

utilizar mensajes .ALR para, 271

Alertas centralizadas, o enviar mensajes de alerta al servidor del Administrador de alertas, 271

alertas DMI (Interfaz de administración del equipo), utilizar con el servidor del Administrador de alertas, 276

alertas DMI, utilizar con el servidor del Administrador de alertas, 276

almacenamiento permanente

definición, 279

archivos .ALR, utilizar para mensajes de Alertas centralizadas, 271

America Online

cliente de correo, compatible con VShield, 94

análisis de heurística doble, 29

arch.

MAILSCAN.TXT como reg. de comp. progr. Expl.email., 253

REG. DE ACTIVIDADES SCREENSCAN.TXT, como reg. ScreenScan, 263

selec. como objetiv. expl., 259

selecc. como objetiv. expl., 217

selecc. como objetiv. explor., 218, 244, 261

VSCLOG.TXT, como registro VirusScan, 229

WEBFLTR.TXT, como registro VShield, 155

WEBINET.TXT, como registro VirusScan, 145

arch. de informe

WEBINET.TXT como, 145

arch. informe

MAILSCAN.TXT como, 253

REG. DE ACTIVIDADES SCREENSCAN.TXT como, 263

VSCLOG.TXT como, 227 a 255

WEBEMAIL.TXT como, 135

WEBFLTR.TXT como, 155 a 156

arch. Reg.

crear con edit.texto, 253

crear con editor de texto, 255

MAILSCAN.TXT como, 253

REG. DE ACTIVIDADES SCREENSCAN.TXT como, 263

VSCLOG.TXT como, 255

arch. registro
crear con editor de texto, 156
crear con editor texto, 135, 145, 155, 227 a 229
VSCLOG.TXT como, 227 a 229
WEBFLTR.TXT como, 155 a 156
WEBINET.TXT como, 145
archivo CENTALRT.TXT
necesario en Alertas centralizadas, 275
archivo de informe
limitar el tamaño de, 118, 136, 146, 156, 229, 255
VSHLOG.TXT como, 117
archivo de registro
crear con editor de texto, 263
información registrada en, 118, 136, 146, 229, 255
limitar el tamaño de, 118, 136, 146, 156, 229, 255
archivo informe
VSHLOG.TXT como, 118
archivo registro
crear con editor texto, 117 a 118
VSHLOG.TXT como, 117 a 118
WEBEMAIL.TXT como, 135
archivos
infectados
eliminar, 112 a 115, 129 a 131, 142 a 143, 223 a 225, 247 a 248
limpiar, 112 a 115, 129 a 131, 142 a 143, 223 a 225, 247 a 248
limpiar cuando VirusScan no puede hacerlo, 63
mover, 112 a 115, 129 a 131, 142 a 143, 223 a 225, 247 a 248
seleccionar como objetivos de exploración, 243 a 246
VSCLOG.TXT, como reg. VirusScan, 255
VSCLOG.TXT, como registro VirusScan, 227
VSHLOG.TXT, como registro VShield, 117 a 118
WEBEMAIL.TXT, como registro VShield, 135
WEBFLTR.TXT, como registro VShield, 156
Archivos COMMAND.COM, infecciones de virus en, xvii
archivos de datos
comunes, entregados con SecureCast, 307
archivos de documentos, agentes de transmisión de virus, xix
archivos de hojas de cálculo, infectados con virus, xix
archivos de Microsoft Office, como agentes para transmisión de virus, xix
archivos del sistema, como agentes para transmisión de virus, xvii
archivos Excel, como agentes para transmisión de virus, xix
archivos infectados
eliminar
incluir en el archivo de registro, 118, 136 a 137, 146
eliminar los virus de los, 61
limpiar cuando VirusScan no puede hacerlo, 63
mover, 114, 130, 143
incluir en el archivo de registro, 118, 136 a 137, 146
uso de la carpeta de cuarentena para aislar, 114, 130, 143

archivos Word, como agentes para transmisión de virus, xix

arranque en caliente, utilización ineficaz para borrar virus, xvii

asistente configuración

utilizar, 94, 99 a 104

asistente de configuración

iniciar, 99

opciones del módulo Exploración de correo electrónico, seleccionar con, 101

opciones del módulo Exploración de transferencias, selección con, 102

opciones del módulo Exploración del sistema, seleccionar con, 100

opciones del módulo Filtro de Internet, seleccionar con, 103

Asistente, botón del cuadro de diálogo Propiedades de VShield, 99

Ayuda

abrir desde la Consola, 204

ayuda en línea

abrir desde la Consola, 204

B

Barra de estado

en la Consola de VirusScan, mostrar y ocultar, 202

Barra de estado

en el menú **Ver**, 202

Barra de herramientas

en la Consola de VirusScan, mostrar y ocultar, 202

Barra de herramientas

en el menú **Ver**, 202

Barra de título

en la Consola de VirusScan, mostrar y ocultar, 202

Barra de título

en el menú **Ver**, 202

Basic, como lenguaje de programación de virus de macro, xix

Biblioteca de información sobre virus, conexión desde VirusScan, 78 a 80

BIOS

como modo de alerta en el explorador VShield en los sistemas de Windows 95 y Windows 98, 113

posible incompatibilidad de VirusScan con características antivirus de, 67

bloques arranque

explor., 221

BOOTSCAN.EXE

utilización con un disco de emergencia, 62

Virus "Brain", xv

bromas, como cargas destructivas, xvi

C

caballos de Troya, definición, xv

caídas del sistema, atribuibles a virus, 61

carga destructiva, definición, xvi

carpeta de cuarentena, usar para aislar archivos infectados, 114, 130, 143

carpetas

selec. como objetiv. expl., 259

selecc. como objetiv. expl., 217

selecc. como objetiv. explor., 218, 244, 261

cc

Mail

cliente de correo electrónico compatible con VShield, 94

conexión y exploración de los buzones de correo de las versiones 6.0, 7.0 y 8.0, 257

seleccionar las opciones correctas para
en el asistente de configuración, 101
en el cuadro de diálogo de propiedades de exploración del correo electrónico, 124
clases de Java
como software perjudicial, xx a xxi
distinción entre virus y, xxi
clic con botón derecho
utiliz. para mostrar menús acceso dir. en Consola VirusScan, 202
cliente para el Administrador de alertas
configurar, 272 a 276
describir y utilizar en el software de VirusScan, 270 a 271
clientes de correo electrón. POP-3, seleccionar opciones para
en el asistente configur., 101
clientes de correo electrónico MAPI (Interfaz de programación de aplicaciones de mensajería)
seleccionar en el asistente de configuración, 102
seleccionar en el cuadro de diálogo de propiedades de exploración del correo electrónico, 124
clientes de correo electrónico POP-3, seleccionar opciones para
en el cuadro de diálogo Exploración de correo electrónico, 125
clientes de correo electrónico SMTP
seleccionar opciones para
en el asistente configur., 101
en el cuadro de diálogo de propiedades de exploración del correo electrónico, 125
componente de programa de Exploración de correo electrónico, respuestas predeterminadas cuando se detecta un virus, 76
componentes, incluidos con VirusScan, 31 a 36
comprobar la instalación, 58
Conectar a unidad de red, 280
configur.
de VShield
en el módulo Explor. correo electr., 122 a 138
en el módulo Explor. de sistema, 105
en el módulo Explor. transf., 138 a 147
configurac.
de VShield
en el módulo Explor. de sistema, 122
configuración
componente de programa de correo electrónico, 240 a 256
de ScreenScan, 257 a 264
de VShield
en el módulo Exploración de correo electrónico, 122 a 138
en el módulo Exploración de transferencias, 138 a 147
en el módulo Filtro de Internet, 148 a 156
en el módulo Seguridad, 156 a 158
utilizar el asistente, 94, 99 a 104
seleccionar opciones para VirusScan en la Consola, 216 a 236
configuración de sesión
incluir en el archivo de registro, 118, 136 a 137, 146

conflictos del software, como causa potencial de los problemas relacionados con equipos, 66
Consola
barra de estado, mostrar y ocultar, 202
barra de herramientas en, mostrar y ocultar, 202
barra de título, mostrar y ocultar, 202
comandos disponibles en, 203 a 204
configuración de tareas en, 203, 216 a 236
copiar y pegar tareas en, 203
crear nuevas tareas en, 203, 207, 211
definición de tarea de exploración en, 202
desactiv. y activar tareas desde, 204
desactivar y activar de tareas desde, 203
descripción general de, 203 a 204
detención tareas desde, 204
ejecución necesaria para iniciar tareas explor., 214
eliminar tareas desde, 203
finalidad de, 199
iniciar, 200
iniciar tareas desde, 203
opciones de acción para VirusScan, configurar desde, 222 a 227
opciones de detección para VirusScan, configuración desde, 217 a 222
opciones de exclusión para VirusScan, configuración desde, 231 a 234
opciones de informe para VirusScan, configurar desde, 227 a 231
opciones de seguridad para VirusScan, configurar desde, 234 a 236
posibles aplicaciones de, 199
programar y activar tareas en, 203, 211 a 214
tareas predeterminadas incluidas con, 205
ventana, elementos de, 202
Consola de VirusScan, 203 a 204
barra de estado, mostrar y ocultar, 202
barra de herramientas en, mostrar y ocultar, 202
barra de título, mostrar y ocultar, 202
configuración de tareas en, 203, 216 a 236
copiar y pegar tareas en, 203
crear nuevas tareas en, 203, 207, 211
desactivar y activar de tareas desde, 203
descripción general de, 203 a 204
eliminar tareas desde, 203
finalidad de, 199
iniciar, 200
iniciar tareas desde, 203
opciones de acción para VirusScan, configurar desde, 222 a 227
opciones de detección para VirusScan, configuración desde, 217 a 222
posibles aplicaciones de, 199
programar y activar tareas en, 203, 211 a 214
tareas predeterminadas incluidas con, 205
ventana, elementos de, 202
Consola VirusScan
desactiv. y activar tareas desde, 204
detención tareas desde, 204
ejecución necesaria para iniciar tareas explor., 214
contenido del archivo de registro, 118, 136, 146, 229, 255
contraseña, seleccionar
en el módulo Seguridad de VShield, 157
para VirusScan en la Consola, 235

controles ActiveX
como software perjudicial, xx a xxi
detectar con el módulo Filtro de Internet de VShield, 148
distinción entre virus y, xxi
copia de seguridad
estrategias, 280 a 281
copia de seguridad duplicada, 278
Copiar
del menú **Edición**, 203
copias de seguridad
automáticas, 279
dónde guardarlas, 280
frecuencia, 281
por qué son necesarias, 278
correo electrón.
software de clientes
seleccionar en el asistente configur., 101
correo electrónico
como agente para transmisión de virus, xix
software de clientes
compatible con VShield, 93
seleccionar en el cuadro de diálogo de propiedades de exploración de correo electrónico, 123 a 129
costes de los daños por virus, xiii a xiv
CTRL+ALT+DEL, utilización ineficaz para limpiar virus, xvii
Cuarentena, 283

D

daños de los virus, xiii
cargas destructivas, xvi
definiciones
tarea, 202
virus, xiii
Desactivar
en el menú **Tarea**, 204
descripción general, de la Consola de VirusScan, 203 a 204
descripciones, de componentes de programa VirusScan, 31 a 36
detecc.
opción
agreg. objetiv. expl. ScreenScan, 259
opciones
agreg. objetiv. expl., 217
agreg. objetiv. expl. ScreenScan, 259
agreg. objetiv. explor., 218, 261
detección
opciones
agreg. objetiv. explor., 244
configurar para el módulo Exploración de correo electrónico, 123 a 129
configurar para el módulo Exploración de sistema, 106 a 112
configurar para el módulo Exploración de transferencias, 139 a 142
configurar para el módulo Filtro de Internet, 148 a 152
eliminación de objetivos de exploración, 219, 260
seleccionar de VirusScan en la Consola, 217
seleccionar en el componente de programa Exploración de correo electrónico, 242 a 246
detecciones, falsas, identificación, 67
Detener
en el menú **Tarea**, 204

disco de emergencia
crear
en un equipo no infectado, 62
utilización de BOOTSCAN.EXE en, 62
utilización para reiniciar el sistema, 62
discos
de unidades
como medio para transm. de virus, xvi a xvii
selec. como objetiv. expl., 259
selecc. como objetiv. expl., 217
selecc. como objetiv. explor., 218, 244, 261
disfrazar infecciones de virus, xviii
disquetes
papel en expans. de virus, xvii
papel en expansión de virus, xvi
distribución de VirusScan
electrónicamente y en disco CD-ROM, 39

E

elementos de la ventana, en la Consola de VirusScan, 202
elementos hostiles
clases de Java y controles ActiveX como, xx a xxi
distinción entre virus y, xxi
eliminador
acciones disponibles cuando VirusScan no tiene ninguna, 63
Eliminar
en el menú **Tarea**, 203
Enterprise SecureCast, 305
cancelación de suscripción, 319
características, 307
instalación, 319
recursos de soporte para, 320
requisitos del sistema para, 308
solución de problemas, 319
equipo no infectado, utilización para crear un disco de emergencia, 62
estadísticas
mostradas en el cuadro de diálogo Estado de VShield, 164
para tarea de exploración, 214 a 215
estado
comprobar de tareas de exploración, 214 a 215
comprobar VShield, 164
Eudora y Eudora Pro
clientes de correo electrónico compatibles con VShield, 94
Exchange
cliente de correo electrónico compatible con VShield, 94
explor. heurística
definición, 112, 140 a 141, 220, 244, 261
exploración heurística
definición, 29, 110, 127
extensiones de nombre de archivo
uso para identificar archivos vulnerables, 288
extensiones de programa, designación como objetivos de exploración, 288
extensiones, usarlas para identificar objetivos de exploración, 288

F

fallos, cuándo no son atribuibles a virus, 66
falsas detecciones, identificación, 67
fecha y hora, incluidas en el archivo de registro, 118, 136, 146

firmas de códigos
utilización por los virus, xviii
firmas, utilización para detección de virus, xviii
formato militar de hora, uso para programar tareas de exploración, 213

G

gusanos, definición, xv

H

hacer clic con el botón derecho del ratón
utilizar para mostrar los menús de acceso directo de VShield, 159
historia de los virus, xiii a xxii

I

información sobre archivos, ver, 78 a 80
Inicio
en el menú **Tarea**, 203
inicio automático, valor para tarea de exploración, 222
inicio rápido para la configuración VShield, 94, 99 a 104
instalación
cancelar si se detecta un virus durante, 61
comprobar la efectividad de, 58
Internet
clientes de correo electrónico, seleccionar
en el asistente de configuración, 101
en el cuadro de diálogo de propiedades de exploración del correo electrónico, 124
expansión de virus a través de, xix
Internet Explorer
como visualizador compatible con VShield, 93
Internet Relay Chat
como agente para transmisión de virus, xxi

L

línea de comandos de VirusScan
utilización al arrancar con un disco de emergencia, 62
lista de tareas
tareas predeterminadas en, 202
Lista de virus
en el menú **Ver**, 204
Lotus cc
Mail
cliente de correo electrónico compatible con VShield, 94
conexión y exploración de los buzones de correo de las versiones 6.0, 7.0 y 8.0, 257
seleccionar las opciones correctas para
en el asistente de configuración, 101
en el cuadro de diálogo de propiedades de exploración del correo electrónico, 124

M

MAILSCAN.TXT, como arch. informe de comp. progr. Explor.email., 253
memoria
explor. como parte de una tarea explor., 221
infecciones virus en, xvi a xvii
mensajes sonoros de alerta, emitir, 116, 134, 144, 154, 227

menú Archivo
Ver registro de actividades, 230
menú **Edición**
Copiar, 203
Pegar, 203
menú **Tarea**
Activar, 203
Desactivar, 204
Detener, 204
Eliminar, 203
Inicio, 203
Nueva tarea, 203, 207
Propiedades, 203
menú **Ver**
Barra de estado, 202
Barra de herramientas, 202
Barra de título, 202
Lista de virus, 204
menús acceso dir.
utiliz. en ventana Consola VirusScan, 202
menús context.
utiliz. en ventana Consola VirusScan, 202
menús de acceso directo
utilizar con VShield, 159
menús, acceso dir.
utiliz. en ventana Consola VirusScan, 202
menús, acceso directo
utilizar desde la bandeja del sistema de VShield, 159
Microsoft
archivos de Word y de Excel, como agentes para transmisión de virus, xix
Exchange, Outlook y Outlook Express, clientes de correo electrónico compatibles con VShield, 94
Internet Explorer
como visualizador compatible con VShield, 93
Visual Basic, como lenguaje de programación de virus de macro, xix
modo de alerta
BIOS, 113
módulo Explor. correo electr.
config., 122 a 138
Módulo Explor. de sistema
configurar, 105 a 122
Módulo Explor. transf.
config., 138
Módulo Explor. transfer.
config., 147
módulo Exploración de correo electrónico
configurar
utilizar el asistente de configuración, 101
utilizar el cuadro de diálogo Propiedades de VShield, 122 a 138
Módulo Exploración de sistema
configurar
utilizar el asistente de configuración, 100
módulo Exploración de sistema
configurar
utilizar el cuadro de diálogo Propiedades de VShield, 105 a 122
opciones de respuesta predeterminadas para, 68 a 71
módulo Exploración de transfer.
opciones de respuesta predetermin. para, 73 a 74

Módulo Exploración de transferencias
configurar
utilizar el asistente de configuración, 102
módulo Exploración de transferencias
configurar
utilizar el cuadro de diálogo Propiedades de VShield, 138 a 147
Módulo Filtro de Internet
configurar, 148 a 156
utilizar el asistente de configuración, 103
opciones de respuesta predeterminadas para, 74
módulo Filtro de Internet
configurar
utilizar el cuadro de diálogo Propiedades de VShield, 148 a 156
módulo Seguridad
configurar, 156 a 158
mutación de virus, definición de, xviii

N

Netscape Navigator y Netscape Mail
como visualizador y cliente de correo electrónico compatibles con VShield, 93
nombre de usuario, incluido en el archivo de registro, 118, 136, 146
Nueva tarea
en el menú **Tarea**, 203, 207
nueva tarea de exploración, crear, 203, 207 a 211

O

objetiv. Expl.
agreg., 259
objetiv. expl.
agreg., 217 a 259
objetiv. explor.
agreg., 218, 261
objetiv.explor.
agreg., 244
objetivos de exploración
eliminar, 219, 260
objetos, Java y ActiveX
como software perjudicial, xx a xxi
opciones
componente de programa Exploración de correo electrónico
Acción, 246 a 249
Alerta, 249 a 253
configurar, 240 a 256
Detección, 242 a 246
Informe, 253 a 256
módulo Explor. correo electr., config., 122 a 138
módulo Explor. de sistema, configurar, 105 a 122
módulo Explor. transf., configurar, 147
módulo Explor. transfer., config., 138
módulo Filtro de Internet, configurar, 148 a 156
módulo Seguridad, configurar, 156 a 158
ScreenScan, configurar, 257 a 264
VirusScan
Acción, 222 a 225
Alerta, 225 a 227
configurar, 216 a 236
Detección, 217
Exclusión, 231 a 234
Informe, 227 a 231
Seguridad, 234 a 236

VirusScan Clásico

Informe, 180

VShield, seleccionar con el asistente configuración, 94, 99 a 104

opciones de acción, seleccionar

en el componente de programa Exploración de correo electrónico, 246 a 249

en el módulo Exploración de correo electrónico, 129 a 131

en el módulo Exploración de sistema, 112 a 115

en el módulo Exploración de transferencias, 142 a 143

en el módulo Filtro de Internet, 153

para VirusScan en la Consola, 222 a 225

opciones de Alerta, seleccionar

en el componente de programa Exploración de correo electrónico, 249 a 253

en el módulo Exploración de correo electrónico, 132 a 135

en el módulo Exploración de sistema, 115 a 117

en el módulo Exploración de transferencias, 144 a 145

en el módulo Filtro de Internet, 153 a 155

para VirusScan en la Consola, 225 a 227

opciones de exclusión, seleccionar

para el módulo Exploración de sistema, 120 a 122

para VirusScan en la Consola, 231 a 234

opciones de informe, seleccionar

en el componente de programa Exploración de correo electrónico, 253 a 256

en el módulo Exploración de correo electrónico, 135 a 138

en el módulo Exploración de sistema, 117 a 119

en el módulo Exploración de transferencias, 145 a 147

en el módulo Filtro de Internet, 155 a 156

para VirusScan en la Consola, 227 a 231

opciones de respuesta

configuración

en el módulo Exploración de correo electrónico, 129 a 131

para el módulo Exploración de sistema, 112 a 115

para el módulo Exploración de transferencias, 142 a 143

para el módulo Filtro de Internet, 153

para VirusScan en la Consola, 222 a 225

elegir

cuando el componente de programa de Exploración de correo electrónico detecta un virus, 76 a 78

cuando el módulo Exploración de correo electrónico detecta un virus, 71 a 72

cuando el módulo Exploración de sistema detecta un virus, 68 a 71

cuando el módulo Exploración de transfer. detecta un virus, 73 a 74

cuando el módulo Filtro de Internet detecta objetos nocivos, 74

cuando VirusScan detecta un virus, 74 a 76

opciones de seguridad

seleccionar de VirusScan en la Consola, 234 a 236

opciones informe, selecc.

en VirusScan Clásico, 180

operaciones de exploración, decidir cuándo hay que empezar, 65

origen de los virus, xiii a xxii
Outlook y Outlook Express
clientes de correo electrónico compatibles con VShield, 94
distinguir entre, 102

P

página Detección
en el componente de programa Exploración de correo electrónico, 242 a 246
en el módulo Exploración de correo electrónico, 123 a 129
en el módulo Exploración de sistema, 106 a 112
en el módulo Exploración de transferencias, 139 a 142
en el módulo Filtro de Internet, 148 a 152
para VirusScan en la Consola, 217 a 222
páginas de propiedades
protección y desprotección, 158, 235
panel de control, VirusScan
abrir, 266
descripción, 265
seleccionar opciones para, 267 a 269
pánico, evitarlo si su sistema sufre una infección, 61
Papelera de reciclaje, excluida de las operaciones de exploración, 231
Pegar
del menú **Edición**, 203
predeterminadas
objetivos de exploración, 288
problemas del equipo, atribuibles a virus, 61
programa, componentes incluidos con VirusScan, 31 a 36
programas ejecutables
como agentes para transmisión de virus, xvii
Propied.
módulo Explor. correo electr.., config. para, 122
Propiedades
configurar para VirusScan, 216 a 236
módulo Explor. correo electr., config. para, 138
módulo Explor. de sistema, configurar para, 105 a 122
módulo Explor. transf., config. para, 138 a 147
módulo Filtro de Internet, configurar para, 148 a 156
módulo Seguridad, configurar para, 156 a 158
VShield
configurar con asistente configuración, 94, 99 a 104
Propiedades
en el menú **Tarea**, 203

Q

Qualcomm Eudora y Eudora Pro
clientes de correo electrónico compatibles con VShield, 94

R

RAM
explor. como parte de una tarea explor., 221
infecciones virus en, xvi a xvii
razones para ejecutar VShield, 92
REGISTRO DE ACTIVIDADES DE SCREENSCAN.TXT, como arch. informe ScreenScan, 263

reiniciar
con CTRL+ALT+DEL, utilización ineficaz para borrar virus, xvii
con el disco de emergencia, 62
reiniciar, con el disco de emergencia, 62
requisitos del sistema
para VirusScan, 39
SecureCast, 308
respuestas, predeterminadas, en caso de infección por virus, 61
resultado
estado de las tareas de exploración, 214 a 215
resultados
mostradas en el cuadro de diálogo Estado de VShield, 164
resumen de sesión
incluir en el archivo de registro, 118, 136 a 137, 146

S

salir de VShield, 159 a 164
sector de arranque maestro (MBR), posibilidades de infección por virus, xvi
SecureCast
archivos de datos comunes que se reciben con, 307
características, 307
Enterprise SecureCast, 305
cancelación de suscripción, 319
instalación, 319
solución de problemas, 319
recursos de soporte para, 320
requisitos del sistema, 308
utilización para actualizar el software, 305
seguridad
contraseña, seleccionar, 158, 235
servidor
copia de seguridad local de los archivos, 281
sistemas de correo corporativo, seleccionar
en el asistente de configuración, 101
en el cuadro de diálogo de propiedades de exploración del correo electrónico, 124
software antivirus
consecuencias de ejecutar versiones de varios fabricantes, 67
firmas de códigos, utilización para detección de virus, xviii
software perjudicial
carga destructiva, xvi
clases de Java como, xx a xxi
controles ActiveX como, xx a xxi
distinción entre objetos hostiles y virus, xxi
expansión a través de World Wide Web, xix a xxi
tipos
caballos de Troya, xv
gusanos, xv
virus de secuencia de comandos como, xxi
solución de problemas de SecureCast
problemas de registro, 319
problemas de servidor de seguridad, 319
soporte
recursos para SecureCast, 320

T

tarea
agreg. objetiv. explor. a, 244, 261

agregar objetiv. explor. a, 218
asignar nombre, 208
configurar opciones de la Consola de VirusScan, 216 a 236
copiar valores de configuración de una a otra, 203
definición, 202
desactiv. y activar, 204
detener, 204
eliminación de objetivos de exploración, 219, 260
eliminar, 203
escribir horas de programación para, 213
estado, comprobar, 214 a 215
horas e intervalos de programación disponibles para, 212
iniciar, 203
automáticamente, 222
necesario para ejecución de Consola, 214
memoria, explor. como parte de, 221
nueva, crear, 203, 207 a 211
objetiv. expl. para
agreg., 217, 259
objetiv. explor. para
agreg., 259
opciones de acción, configurar, 222 a 227
opciones de detección
seleccionar de VirusScan en la Consola, 217 a 222
opciones de exclusión, configurar
para VirusScan en la Consola, 231 a 234
opciones de informe, configurar
para VirusScan en la Consola, 227 a 231
opciones de registro, configurar
para VirusScan en la Consola, 227 a 231
opciones de seguridad, configurar, 234 a 236
opciones informe, config.
para VirusScan Clásico, 180
pegar valores de configuración de una a otra, 203
predeterminadas, incluidas con la Consola de VirusScan, 205
programación para llevar a cabo, seleccionar, 208
programar y activar, 203, 211 a 214
tarea de exploración
asignar nombre, 208
configurar
opciones de la Consola de VirusScan, 216 a 236
copiar valores de configuración de una a otra, 203
definición, 202
eliminar, 203
escribir horas de programación para, 213
estado, comprobar, 214 a 215
excluir elementos de, 231
horas e intervalos de programación disponibles para, 212
iniciar, 203
automáticamente, 222
nueva, crear, 203, 207 a 211
objetivos para
eliminar, 219, 260
opciones de acción, configurar, 222 a 227
opciones de detección
seleccionar de VirusScan en la Consola, 217

opciones de exclusión, configurar
para VirusScan en la Consola, 231 a 234
opciones de informe, configurar
para VirusScan en la Consola, 227 a 231
opciones de registro, configurar
para VirusScan en la Consola, 227 a 231
opciones de seguridad, configurar, 236
pegar valores de configuración de una a otra, 203
predeterminadas
incluidas con la Consola de VirusScan, 205
programación para llevar a cabo, seleccionar, 208
programar y activar, 203, 211 a 214
tarea expl.
objetiv. para
agreg., 259
tarea expl..
objetiv. para
agreg., 217
tarea explor
iniciar
necesario para ejecución. de Consola, 214
tarea explor.
bloques arranque, explor. como parte de, 221
desactiv., 204
detener, 204
memoria, explor., 221
objetiv. para
agreg., 218, 244, 261
opciones informe, config.
para VirusScan Clásico, 180
tarea exploración
opciones de seguridad, configurar, 234
tareas de exploración
aceleración de, 231
programar y activar
como finalidad de la Consola, 199
posibles aplicaciones de, 199
tareas de exploración en segundo plano, configurar
en el asistente de configuración, 100
en el cuadro de diálogo Propiedades de exploración del sistema, 104 a 122
en ScreenScan, 257 a 264

Temas de Ayuda

del menú **Ayuda**, 204
texto
editor, usar para crear arch. registro, 135, 155 a 229
editor, usar para crear archivo registro, 117 a 118, 145
editor, usar para crear el arch. Reg., 255
editor, usar para crear el arch. registro, 227
editor, usar para crear el archivo de registro, 263
mensajes, utilización para transmisión de virus, xxi
para crear arch. Reg., 253
texto normal, utilización para transmisión de virus, xxi

U

Utilidad de configuración de cliente del Administrador de alertas
configurar, 272 a 276
describir y utilizar, 270 a 271

V

formato de reloj de 24 horas, uso para escribir horas de programación, 213
Ver registro de actividades
en el menú **Archivo**, 230
en el menú **Tarea**, 230
virus
¿por qué preocuparse?, xiv
carga destructiva, xvi
Concept, xix
costes de, xiii a xiv
decidir cuándo hay que iniciar las operaciones de exploración para, 65
definición, xiii
detectar, incluidos en el archivo de registro, 118, 136 a 137, 146
disfrazar infecciones de, xviii
distinción entre objetos hostiles y, xxi
efectos de, xiii, 61
eliminar
antes de la instalación, necesidad y pasos, 61
de los archivos infectados, 61
encriptado, definición de, xviii
expansión a través del correo electrónico y de Internet, xix
falsas detecciones, identificación, 67
firmas de códigos, utilización por, xviii
historia de, xiii a xxii
infección de archivos, xvii
infección sector de arranque, xvi a xvii
lenguaje de secuencia de comandos, xxi
limpiar, incluidos en el archivo de registro, 118, 136, 146
macro, xix
config. de opciones de explor. heurística para, 220
configur. de opciones de explor. heurística para, 110 a 112, 127, 140 a 141, 261
configur. opciones de explor. heurística para, 244
mutación, definición de, xviii
números actuales de, xiii
origen de, xiii a xxii
papel de los equipos informáticos en su expansión, xv
polimórfico, definición de, xviii
programas similares a
caballos de Troya, xv
gusanos, xv
reconocer cuándo los problemas del equipo no son resultado de, 66
respuesta predeterminada a
cuando el componente de programa de Exploración de correo electrónico detecta un virus, 76
cuando VirusScan detecta, 74
cuando VShield detecta, 68 a 74
sigilosos, definición, xviii
ver información acerca de, 78 a 80
Virus "Brain", xv
Virus Concept, introducción, xix
virus de equipos informáticos, origen de, xv
virus de macro
config. de opciones de explor. heurística para, 220

configur. de opciones de explor. heurística para, 110 a 112, 127, 140 a 141, 261

configur. opciones de explor. heurística para, 244

definición y comportamiento, xix

virus Concept, xix

virus de secuencia de comandos, xxi

virus de secuencia de comandos mIRC, xxi

virus encriptados, xviii

virus polimórficos, definición de, xviii

virus que infectan archivos

config. de opciones de explor. heurística para, 220

configur. de opciones de explor. heurística para, 110 a 112, 140 a 141, 261

configur. opciones de explor. heurística para, 244

configuración de opciones de explor. heurística para, 127

definición y comportamiento, xvii

virus sector de arranque, defin. y comportam. de, xvi a xvii

virus sigilosos, definición, xviii

VirusScan

como componente del paquete Active Virus Defense, 27

componentes incluidos con, 31 a 36

configurar tareas de exploración, 216 a 236

descripción de componentes de programa, 31 a 36

descripción general de las características, 25

funciones antivirus BIOS, posible incompatibilidad con, 67

instalación

como la mejor protección contra las infecciones, 61

qué hacer cuando se detecta un virus durante, 61

introducción, 25

métodos de distribución, 39

opciones de Acción

seleccionar en la Consola, 222 a 225

opciones de Alerta

seleccionar en la Consola, 225 a 227

opciones de detección

seleccionar en la Consola, 217

opciones de exclusión

seleccionar en la Consola, 231 a 234

opciones de informe

seleccionar en la Consola, 227 a 231

opciones de registro, elección en la Consola, 227 a 231

opciones de seguridad, seleccionar en la Consola, 234 a 236

páginas de propiedades

Acción, 189222 a 225

Alerta, 225 a 227

Detección, 217 a 222

Exclusión, 231 a 234

Informe, 227 a 231

Seguridad, 234 a 236

panel de control

abrir, 266

descripción, 265

seleccionar opciones para, 267 a 269

respuestas predeterminadas a la detección de virus, 74

ventana principal
utilización para seleccionar la respuesta a la infección, 75
VirusScan Clásico
opciones informe, selecc., 180
Visual Basic, como lenguaje de programación de virus de macro, xix
visualizadores compatibles con VShield, 93
volumen protegido
archivos, 278
VSCLOG.TXT, como arch. informe VirusScan, 227 a 255
VShield
asistente configuración
utilizar, 94, 99 a 104
asistente de configuración
iniciar, 99
componentes incluidos con VirusScan, 31 a 36
cuadro de diálogo Propiedades
botón **Asistente**, 99
módulo Exploración de correo electrónico, 122 a 138
Módulo Exploración de sistema, 105 a 112
Módulo Exploración de transferencias, 138 a 147
Módulo Filtro de Internet, 148 a 156
módulo Seguridad, 156 a 158
desactivar y activar, 159 a 164
descargar de la memoria, 159 a 164
detener y descargar de la memoria, 159 a 164
módulo Explor. correo electr.
config., 122 a 138
Módulo Explor. de sistema
configurar, 105 a 122
Módulo Explor. Transf.
configurar, 138
Módulo Explor. transf.
config., 147
módulo Exploración de correo electrónico
opciones de respuesta predeterminadas para, 71 a 72
Módulo Exploración de sistema
opciones de respuesta predeterminadas para, 68 a 71
Módulo Exploración de transfer.
opciones de respuesta predeterm. para, 74
opciones de respuesta predeterminadas para, 73
Módulo Filtro de Internet
configurar, 148 a 156
opciones de respuesta predeterminadas para, 74
módulo Seguridad
configurar, 156 a 158
qué hace, 91
razones para ejecutar, 92
respuestas predeterminadas a la detección de virus, 68 a 74
visualizadores y clientes de correo electrónico compatibles, 93
VSHLOG.TXT, como archivo de informe VShield, 117 a 118

W

WEBEMAIL.TXT, como arch. registro
VShield, 135

WEBFLTR.TXT, como arch. registro de
VShield, 155

WEBFLTR.TXT, como arch. registro
VShield, 156

WEBINET.TXT, como arch. registro
VirusScan, 145

World Wide Web, como fuente de software
perjudicial, xix a xxi