ÍNDICE

1. DIAGNÓSTICO

Las incidencias relacionadas con la seguridad y la confianza de los usuarios en la Red son un factor crítico que condiciona el desarrollo de la Sociedad de la Información en España, retrasando la adopción y extensión de servicios a través de Internet, como el comercio electrónico, la administración electrónica o la banca online.

Usos de internet en los hogares.

En los estudios de la Seguridad de la Información y eConfianza en los hogares españoles, realizados por INTECO, se aprecia que cada vez es mayor el número de hogares que acceden a Internet a través de Banda Ancha. Del mismo modo es notable el crecimiento en la frecuencia de uso, llegando al 26,1% de usuarios habituales de Internet que le dedican más de 20 horas semanales siendo el correo electrónico (99,3%) y la búsqueda de información (79,8%) los servicios más usados.

Destacan también usos como el chat (66,6%), la banca online (63,3%), los pagos por Internet (26,9%) o la videoconferencia (19,8%). Se constata también una amplia experiencia en Internet, ya que el 90% afirma utilizarla desde hace al menos 2 años y el 65,4% desde hace más de cinco años.

Otro dato a destacar son los usuarios que utilizan programas de descarga de archivos, que alcanza el 46%, dejando desatendido el ordenador al menos una vez al día.

Herramientas de seguridad en el hogar.

La tendencia actual de creación de códigos maliciosos tiene un objetivo netamente lucrativo, lo que redunda en la programación de *malware* de riesgo alto. Aquellos tiempos en el que la motivación de los creadores de códigos maliciosos era principalmente por el reconocimiento público, ha dado paso a grupos mafiosos organizados cuyo único fin es el económico. Al infectar los equipos de los usuarios los atacantes toman el control de los sistemas, centrándose principalmente en la captura de credenciales bancarias, y en la utilización colectiva de los equipos comprometidos – lo que se conoce como redes zombis – con diferentes fines maliciosos; envío de correo basura, ataques de denegación de servicio a páginas Web, fraude en buscadores y publicidad en línea.

Los datos del estudio revelan que en durante el escaneo de los equipos, mediante la herramienta proporcionada por INTECO, casi 8 de cada 10 equipos (77,1%) mantiene uno o más códigos maliciosos en el ordenador con el que se accede a Internet.

Por ello, es hoy más necesario que nunca que los usuarios sean conscientes de la utilidad de las herramientas de seguridad como los antivirus, cortafuegos, antiespías, etc. Con esa premisa a lo largo de esta guía se da un repaso de las principales herramientas de seguridad que es recomendable utilizar en un entorno doméstico, que son y para qué sirven. Además de un completo listado de herramientas gratuitas, acompañado por manuales prácticos, para facilitar al usuario su instalación y uso básico.

Para completar el catálogo y para que los internautas tengan conocimiento de todas las herramientas disponibles se listan las opciones comerciales de los diferentes fabricantes de soluciones de seguridad.

Por último, resaltar que aunque estas soluciones informáticas son fundamentales los usuarios deben conocer sus limitaciones. Es imprescindible, para aumentar la seguridad, acompañarlas con unos buenos hábitos, que garanticen un uso responsable y seguro de las nuevas tecnologías.

2. HERRAMIENTAS: DEFINICION

2.1. ANTIVIRUS

Qué son:

Son herramientas diseñadas para detectar, bloquear y eliminar virus informáticos y otros programas maliciosos.

Existen dos tipos de antivirus: de escritorio y en línea.

Los antivirus de escritorio son aquellos que se instalan en el ordenador de forma local y protegen al equipo de ataques llegados a través de Internet y del correo electrónico así como de dispositivos extraíbles. Trabajan incluso cuando el ordenador no está conectado a Internet y deben ser actualizados para mantener su efectividad.

Por su parte, los antivirus en línea son herramientas que no necesitan ser instaladas en nuestro ordenador y se accede a ellos mediante el navegador y solo es necesario disponer de conexión a Internet, además de un navegador actualizado.

No sustituyen al antivirus "tradicional" que se instala en nuestro ordenador, pero sí que permiten realizar análisis en cualquier momento y desde cualquier lugar. También permiten verificar nuestro ordenador con un antivirus que no sea el que tenemos instalado, que en determinadas ocasiones podría estar comprometido o no ser efectivo. Una de sus ventajas más atractivas es que suelen ser gratuitos.

Sin embargo, lo cierto es que son menos eficaces que los antivirus de escritorio ya que no son tan completos y no aportan una protección permanente (cuando se cierra el navegador dejan de funcionar). Además, sólo actúan en el ordenador dejando sin protección áreas sensibles del sistema o el habitual tráfico de correos electrónicos.

Los antivirus online complementan a los antivirus de escritorio pero no los sustituyen.

Para qué sirven:

Vigilan todas las entradas y salidas de información a nuestro ordenador como son los dispositivos de almacenamiento y las vías de comunicación con Internet, como el correo electrónico, las páginas web o la mensajería instantánea.

De qué protegen:

Protegen a un ordenador de la posible infección por virus y otros programas maliciosos, y en caso de infección proporcionan mecanismos para la limpieza del fichero o ficheros infectados, además de otras.

Escenarios de aplicación:

- Están indicados para todo tipo de sistemas de información basados en equipos informáticos y de comunicaciones.
- Son compatibles con las diferentes plataformas existentes en el mercado, como Windows, Linux o MAC.

- Existen productos antivirus para el hogar y para el entorno empresarial, así como para servicios y sistemas específicos, como servidores de correo electrónico o web.

Recomendaciones y buenas prácticas:

- Actualice la herramienta antivirus con frecuencia para conseguir una protección eficaz.
- Active la actualización automática en la configuración del producto.
- Verifique cada mensaje nuevo de correo antes de abrirlo, sobre todo los que contengan ficheros adjuntos y los de origen sospechoso.
- Evite la descarga e instalación de programas desde sitios web que no ofrezcan garantías.
- En algunos casos, puede que le resulte útil considerar el uso de los servicios de empresas que ofrecen seguridad gestionada o implantan herramientas de seguridad.

2.2. ANTIESPIAS

Qué son:

Son herramientas que detectan y bloquean la instalación y ejecución de programas destinados a recopilar información sobre su actividad con el ordenador y sus hábitos de navegación, sin su conocimiento, con objetivos publicitarios o de robo de información. Escanean y eliminan de los sistemas, el software que espía nuestros hábitos y conexiones.

Para qué sirven:

- Controlan las descargas de ficheros desde Internet o desde el correo electrónico, analizando si se trata de un software espía.
- Impiden el control remoto de su equipo por personas no autorizadas mediante la instalación de estos programas en su ordenador.
- Escanean los dispositivos de almacenamiento y el software de sistema para detectar software espía.

De qué protegen:

- Protegen la privacidad de los usuarios contra cualquier software que espía sus contenidos y su actividad (conexiones, páginas web que visita…).
- Impiden que se pueda llevar un registro remoto de su actividad, hábitos o uso de su ordenador.
- Evitan la pérdida de productividad debido a la ralentización de los sistemas que infectan.

Escenarios de aplicación:

Estas herramientas están indicadas para todo tipo de usuarios de Internet y especialmente para aquellos que hacen un uso intensivo de búsquedas, comercio electrónico, suscripción a foros y boletines, banca electrónica, etc.

Recomendaciones y buenas prácticas:

- Actualice la herramienta con frecuencia para garantizar una protección efectiva.
- Verifique la procedencia y fiabilidad de los ficheros adjuntos en su correo electrónico.
- No descargue ficheros (ejecutables, salvapantallas, software…) que procedan de fuentes desconocidas.
- Considere los servicios de empresas que ofrezcan seguridad gestionada o la implantación de herramientas de seguridad.

2.3. CORTAFUEGOS

Qué son:

Los cortafuegos o firewalls personales son programas que se encargan de controlar, permitiendo o denegando las conexiones entrantes y salientes de un ordenador. Las conexiones ocurren de forma general cuando nos encontramos conectados a Internet o una red local.

Establecen una barrera entre su ordenador y la red a la que está conectado, bloqueando el tráfico, discriminando entre aplicaciones permitidas y las que no lo están. Ofrece diferentes niveles de seguridad en función del uso y conocimientos del usuario.

Para qué sirven:

- Evitan ataques bloqueando accesos y conexiones no autorizadas, impidiendo que se produzcan. Complementa las defensas antivirus, anti software malicioso, etc.
- Bloquean el tráfico basándose en un esquema de aplicaciones fiables - no fiables.
- Ofrecen varios niveles de seguridad pre configurados para satisfacer las distintas necesidades de seguridad del usuario
- Proporcionan información sobre los intentos de ataque.

De qué protegen:

- De los accesos no permitidos a través de la red.
- De los intentos automatizados de acceso a su equipo que producen saturación de los recursos, impidiendo el buen funcionamiento del mismo.
- Permiten controlar las conexiones salientes de la máquina evitando que el software malicioso que haya conseguido instalarse en un ordenador pueda establecer conexiones hacia el exterior. También es una forma de detectar cualquier actividad sospechosa en el ordenador.

Escenarios de aplicación:

Están indicados para todo tipo de equipos que se conecten a redes y que requieran una protección a nivel de ordenador personal.

Recomendaciones y buenas prácticas:

- Instale cortafuegos para proteger su equipo frente a accesos externos y manténgalo actualizado.
- Un cortafuegos no es una solución para proteger sus equipos de virus y software espía o «spyware». Debe de complementarla con herramientas antivirus y antiespías.
- Identifique las aplicaciones confiables y los usuarios autorizados.
- Revise los mensajes y el registro de actividad del cortafuegos con frecuencia.
- Controle no sólo las conexiones salientes sino también las entrantes.
- Considere los servicios de empresas que ofrezcan seguridad gestionada, pruebas de seguridad o la implantación de herramientas de seguridad.

2.4. CONTROL PARENTAL

Qué son:

Se trata de un software que es capaz de bloquear, restringir o filtrar el acceso a determinada información de Internet no apta para niños y adolescentes.

Para qué sirven:

Este software permite restringir distintas opciones con el fin de lograr cierto control sobre el ordenador al que se lo apliquemos, como por ejemplo:

- Establecer un límite de tiempo para el uso del equipo.
- Evitar el uso de determinados juegos.
- Determinar las páginas web bloqueadas para un usuario.
- Limitar el uso de aplicaciones del sistema.
- Llevar a cabo control de informes.

De qué protegen:

Protege a los niños de ciertos contenidos que están en Internet y que pueden ser considerados no aptos para ellos, así como de ciertos servicios en línea que pueden suponer un riesgo para ellos.

Escenarios de aplicación:

Está indicado para todo tipo de ordenadores que se conecten a Internet y que sean utilizados por niños y adolescentes en general.

Recomendaciones y buenas prácticas:

Es necesario establecer permisos en el ordenador donde será instalada la herramienta para evitar que la protección parental pueda ser desactivada.

2.5. ANTI-PHISHING

Qué son:

El phishing es una técnica que combina el spam (envío de correos masivos de forma indiscriminada) y la ingeniería social (tácticas de persuasión que suelen valerse de la buena voluntad y falta de precaución) mediante la cual, el estafador se hace pasar por una empresa de confianza — normalmente una entidad bancaria—, con el fin de obtener información (contraseñas, datos bancarios, etc.) del usuario, con fines lucrativos.

Las herramientas anti-phishing identifican sitios web y mensajes que puedan suponer una amenaza y comprometer la identidad del usuario. Se integran con navegadores y gestores de correo. Estas herramientas suelen presentar también funcionalidades para evitar el spam, especialmente el que contiene correos del tipo phishing.

Para qué sirven:

Evitan el acceso a páginas web no confiables mediante filtros, listas blancas, listas negras y otras técnicas, proporcionando alertas inmediatas sobre sitios web no confiables.

Evitan que nos lleguen mensajes del tipo phishing entre el correo no deseado o spam.

De qué protegen:

- Del robo de contraseñas y datos bancarios.
- De que seamos objeto de estafas por parte de terceros que suplantan la identidad de empresas de confianza (bancos, administración pública…).

Escenarios de aplicación:

Indicado para todo tipo de ordenadores que hacen uso del correo electrónico e Internet. Especialmente indicado para personas que realizan operaciones bancarias a través de páginas web.

Recomendaciones y buenas prácticas:

- Nunca acceda a la banca electrónica haciendo clic en enlaces o utilizando los favoritos del navegador. Escriba siempre la «URL» (por ejemplo: http://www.mibanco.es) de la entidad directamente sobre el navegador.
- Verifique que la página web es segura —empieza por «https://»— y que está certificada — tiene un candado en la parte inferior derecha—. Haciendo doble clic sobre este candado puede confirmar que la web es legítima.
- No acceda a la banca «on-line» desde ordenadores o sitios no confiables (cibercafés, aeropuertos…).
- Utilice siempre contraseñas difíciles de averiguar, especialmente para la banca electrónica.
- Utilice contraseñas específicas para cada servicio / aplicación.
- Mantenga limpio su equipo de virus y otros códigos maliciosos, software malicioso, mediante el uso de herramientas contra el software malicioso actualizadas.
- Si tiene alguna sospecha de estafa, consulte con la entidad bancaria.
- Considere los servicios de empresas que ofrezcan seguridad gestionada o la implantación de herramientas de seguridad.

2.6. PROTECCION WEB

Qué son:

Las herramientas destinadas a la protección web se centran en proteger al usuario y su ordenador de las diversas amenazas que están apareciendo en este medio de comunicación en Internet, como los sitios web infectados, el código malicioso que se incluye en algunas páginas, la ingeniería social, las páginas falsas, el phishing y otros.

Son muchas las amenazas que están apareciendo relacionadas con el uso de los navegadores y la web, y es por ello que los fabricantes de herramientas de seguridad están incluyendo la protección web como un elemento más de sus herramientas de seguridad.

Para qué sirven:

Evita la infección del ordenador a través de la navegación web, la ejecución malicioso en nuestro ordenador que está contenido en las páginas web que visitamos, el robo de datos o la ingeniería social.

De qué protegen:

Protege de todas las amenazas de seguridad que atacan nuestro ordenador a través del web y de la navegación web en general.

Escenarios de aplicación:

Estas herramientas están recomendadas para cualquier usuario que utilice y navegue en Internet, puesto que el riesgo de infección u otros sin esta protección es muy alto.

Recomendaciones y buenas prácticas:

- Mantenga siempre actualizado su navegador.
- Active la configuración de seguridad de su navegador, de forma que le permita navegar pero con una seguridad adecuada.
- No visite páginas o sitios de dudosa reputación, el riesgo asociado a estos sitios de infectarse o ser vulnerado mediante código malicioso es muy elevado.
- Utilice estas herramientas de seguridad siempre en combinación con otras herramientas, como los antivirus o los antiespías. Son un complemento al resto de herramientas de seguridad disponibles.

3. HERRAMIENTAS GRATUITAS

3.1 ANTIVIRUS DE ESCRITORIO

Son programas que se instalan en el sistema y nos ofrecen protección frente a diversas amenazas de software malicioso como virus, gusanos, troyanos... Estos programas detectan amenazas conocidas, amenazas potenciales. La tendencia es proteger de forma integral el sistema, correo electrónico, navegación, ejecución de código oculto...

Estos programas basan parte de su funcionamiento en un "fichero de firmas" de software malicioso, este fichero se actualiza a través de Internet de forma automática para incluir las últimas detecciones de software malicioso.

Avast Home.

Este antivirus, además de la protección estándar, cuenta con módulos de protección para el correo de Internet, escudo de red, mensajería instantánea, Outlook/Exchange, Peer to Peer y protección Web, pudiendo personalizar cada protección por separado, y pudiendo proteger el acceso a la configuración mediante una contraseña. Cada módulo se puede pausar y detener en función de nuestras necesidades.

También desde la configuración podemos modificar valores de la configuración, entre ellos, uno muy interesante son los avisos mediante el servicio de mensajería de Windows, correo electrónico (MAPI y SMTP) o hacia una impresora.

Instalación

Desde la página del programa ***http://www.avast.com/*** (o bien desde este ***link de descarga***), a la pregunta sobre la acción a realizar con el fichero responderemos ***Guardar***, fijamos la carpeta de descarga y guardamos.

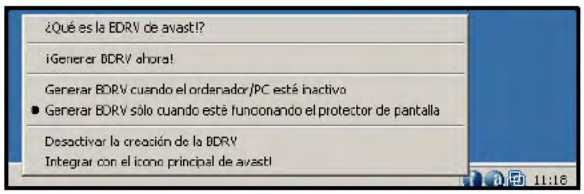
Una vez descargado, ejecutamos el fichero descargado, aparecerá una advertencia de seguridad indicando el posible riesgo.

Ejecutamos el fichero, y seguimos los pasos de instalación. En el paso donde nos muestra un resumen de las opciones de instalación que hemos seleccionado, las comprobamos y si hay alguna opción mal, pulsaremos el

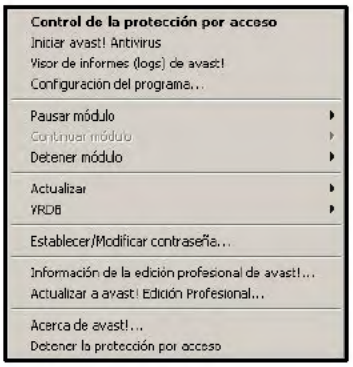
Seguridad informática: Herramientas

(Basado en la guía INTECO)

botón ***Atrás*** y lo corregiremos, en caso de que sea correcto pulsamos la opción ***Siguiente***.



Aparecerán pantallas de progreso de la instalación, cuando el producto esté instalado, aparecerá un ventana en la cual nos permite reiniciar. En el momento de reiniciar, se ejecutará un chequeo previo a la carga del sistema. Al terminar el chequeo y arrancar el sistema muestra una pantalla que nos indica que hemos instalado el antivirus, pulsamos el botón de ***Aceptar*** y aparecen dos iconos de la aplicación... , el derecho muestra el estado de la protección permanente, el izquierdo sirve para generar la base de datos de detecciones, que es lo primero que se debe hacer, hacemos clic derecho sobre el icono de Avast marcado con una i, y de las opciones seleccionamos la opción de ***Generar BDRV ahora***.

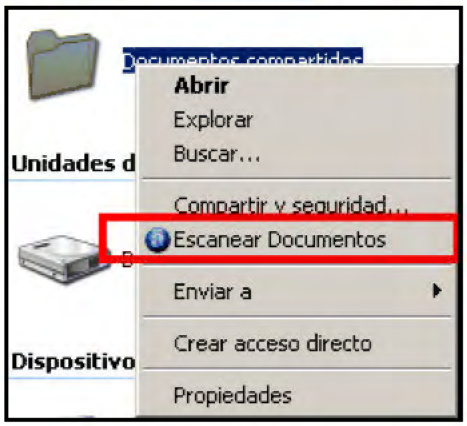


Una vez hecho, nos queda el antivirus instalado y nuestro sistema protegido.

Si queremos cambiar alguna opción, solo tenemos que hacer clic derecho sobre el icono de Avast, marcado con la "a", y seleccionar la opción a modificar. Dentro de estas podemos modificar el alcance de cada protección, modificar la configuración, pausar o detener módulos, proteger la configuración con contraseña, actualizar la base de datos...

Uso Básico

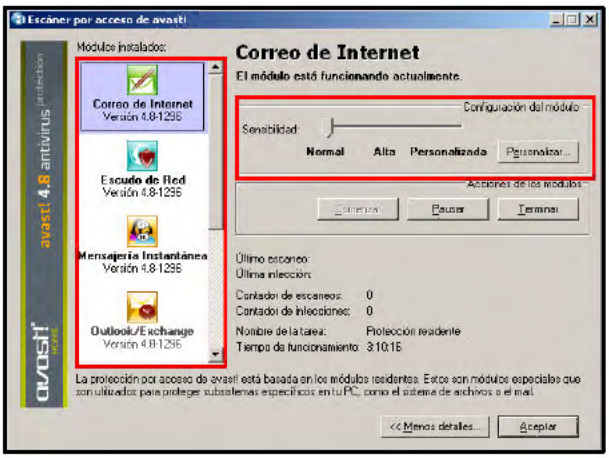
En primer lugar señalamos que los antivirus son funcionales estando instalados (pasos descritos) y actualizados (se hace de forma automática, o podemos forzarlo desde el menú contextual del icono marcado como "a", opción ***Actualizar***, sub opción ***Base de datos***).



Para realizar un escaneo de un fichero, directorio, disco... basta con que abramos la carpeta o unidad que lo contiene y hagamos clic derecho sobre el elemento y seleccionemos del menú contextual la opción ***Escanear Documentos***.

También podemos configurar cada módulo, para ello del menú contextual de la aplicación (clic derecho sobre el icono marcado con "a"), seleccionamos la opción, ***Control de la protección por acceso***, aparece la ventana ***Siguiente***, en ella seleccionamos primero el módulo que vamos a modificar, y después marcamos la sensibilidad de ese control. Cuanta más sensibilidad, más seguridad tendremos, pero perdemos algo de funcionalidad.

Estos niveles se pueden personalizar.



Avira AntiVir Personal.

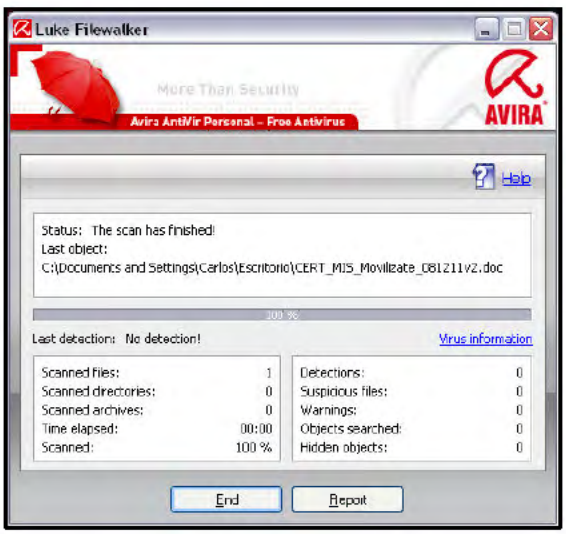
Este antivirus ofrece una protección segura y efectiva, vigilando en todo momento el sistema con un Virus Guard residente que controla los movimientos de archivos, por ejemplo cuando se descargan archivos de Internet, aunque también dispone de integración con el Explorador de archivos, así que con hacer clic derecho en cualquier documento que consideremos sospechoso, podremos analizarlo en búsqueda de software maligno.

Instalación

Desde la página del programa ***http://antivir.es/cms/*** (o bien desde este ***link de descarga***), a la pregunta sobre la acción a realizar con el fichero responderemos ***Guardar***, fijamos la carpeta de descarga y guardamos.

Una vez descargado, ejecutamos el fichero, aparece una advertencia de seguridad indicando el posible riesgo, vamos siguiendo los pasos de la instalación, seleccionamos ***Instalación completa***, la aplicación se instala y cuando termina aparece una ventana en la cual nos indica que ha finalizado.

Según ha terminado, nos pregunta si queremos actualizar la base de datos de virus, , pulsamos el botón de ***SI***, cuando termina, cierra la ventana de actualización y aparece un icono del programa (paraguas rojo abierto, funcionando, cerrado, no funciona)



Uso Básico

El funcionamiento del programa es muy sencillo, para escanear un fichero solo hay que seleccionarlo, dar al botón derecho del ratón y seleccionar ***Scan selected files with antivir*** y nos presentará un informe.

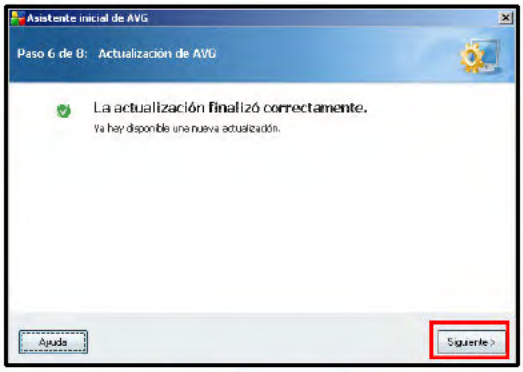
Si se quiere escanear el sistema (o algunas carpetas), vamos a "Mi PC", y seleccionamos el disco que queremos escanear, y el programa realiza el escaneo automáticamente.

AVG Free Antivirus.

Desde la página ***http://free.avg.com/***, (o bien desde este ***link de descarga***), a la pregunta sobre la acción a realizar con el fichero responderemos ***Guardar***, fijamos la carpeta de descarga y guardamos.

Una vez descargado, hacemos doble clic en el icono del fichero para instalarlo....

Se nos muestra una ventana de aviso de seguridad donde nos informa de los riesgos, pulsamos el botón de ***Ejecutar***, y comienza la instalación Seleccionamos el idioma del combo desplegable que aparece en la parte inferior derecha, y aparecerá el saludo y las opciones en español.



El programa nos instala también una barra de seguridad de AVG con varias opciones, podemos instalarla o no, pulsamos ***Siguiente***. Nos aparece el resumen de la instalación, pulsamos en ***Finalizar*** para que la instalación comience realmente. Una vez finalizada aparece la ventana en la que nos informa, pulsamos ***OK***.

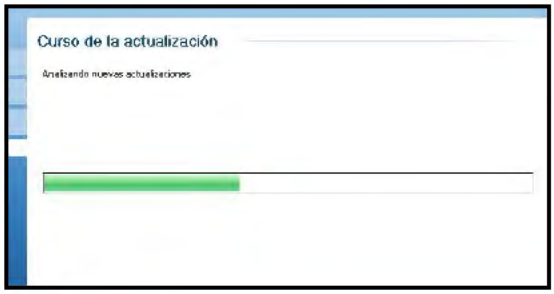
A continuación aparecen una serie de ventanas para configurar otras opciones del programa. La primera que aparece es una que nos informa de la instalación correcta, pulsamos el botón ***Siguiente***. Configuramos la frecuencia de las instalaciones, si queremos un análisis diario y a qué hora, pulsamos siguiente. Nos pide permiso para que las páginas que visitemos y tengan vulnerabilidades pueda reportarlas al servidor para registrarlas, pulsamos ***Siguiente***.

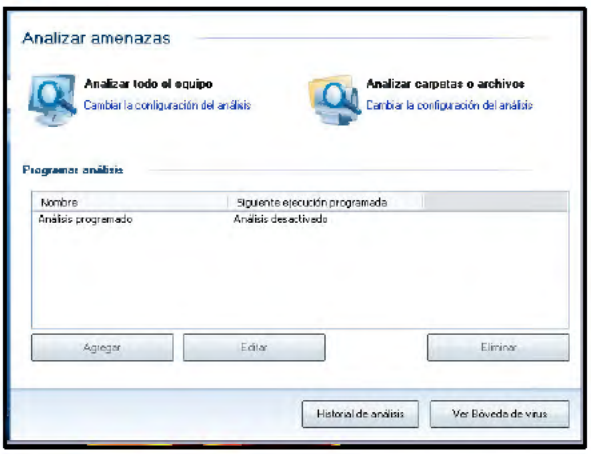
La siguiente ventana nos indica que se va a actualizar el fichero de firmas de virus, pulsamos ***Siguiente***.

Como indicativo de que el antivirus está instalado y funcionando, aparece un icono de colores al lado del reloj.

Uso Básico

El antivirus AVG presenta diferentes funcionalidades. Dentro de las más básicas está realizar análisis del equipo para la búsqueda de virus, en el análisis, se puede seleccionar un análisis completo o un análisis específico de las carpetas o archivos que se desea escanear. Otra funcionalidad es programar análisis del equipo para fechas y horas determinadas, que proporcionará una política de protección, y la actualización de la base de datos de virus y spyware.





Para mantener el antivirus actualizado, se debe actualizar cada cierto tiempo, o mantener las actualizaciones automáticas. Para ello se hará en cada inicio del sistema, o manualmente a través de las actualizaciones.

Ante la descarga de archivos de la red o de cualquier otro fichero anexo en un correo electrónico. Se debe descargar el fichero y analizarlo, pulsando sobre el botón derecho encima del archivo. Si se quiere analizar una carpeta y su contenido se realiza pulsando encima de la carpeta con el botón derecho y pulsamos en.

Para comprobar que nuestro antivirus está activado. Podemos verlo en el "área de notificación". Donde se muestra el siguiente icono.

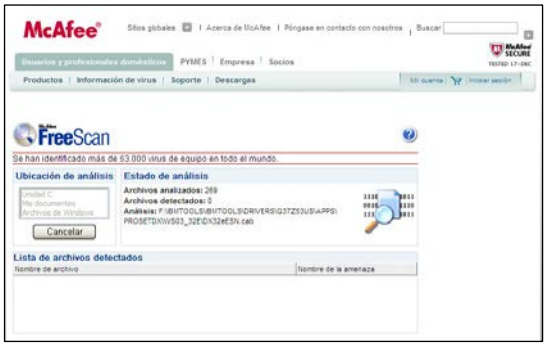
3.2 ANTIVIRUS EN LINEA

Estos antivirus no se instalan en el PC como un programa convencional, sino que se accede mediante un navegador web. El tiempo de escaneo varía en función de la velocidad de la conexión, la carga momentánea de los servidores o el volumen de datos que se quiera rastrear. La mayoría de estos servicios descargan un subprograma (ActiveX o Java), por lo que la primera vez que se accede tardan unos minutos en arrancar.

Los antivirus en línea no evitan que el ordenador se quede infectado. Pero son útiles para realizar un segundo análisis, cuando se sospecha que el ordenador puede estar infectado, pero el antivirus de escritorio no detecta nada extraño.

McAffe Free Scan.

Se va a la página del antivirus (http://es.mcafee.com/root/mfs/default.asp), se pincha en "analizar ahora", entonces el antivirus solicita la instalación de un control ActiveX para poder funcionar,



Cuando se instala (puede tardar unos minutos), aparece la pantalla inicial del antivirus, donde se puede elegir escanear diferentes lugares (Unidad C, carpeta Mis Documentos o Archivos de la carpeta Windows).

Cuando finaliza presenta un informe de los ficheros infectados.

Panda Active Scan.

Es un antivirus que escanea todo el equipo por defecto, detectando todo tipo de software malicioso y vulnerabilidades, además realiza la desinfección (previo registro gratuito).

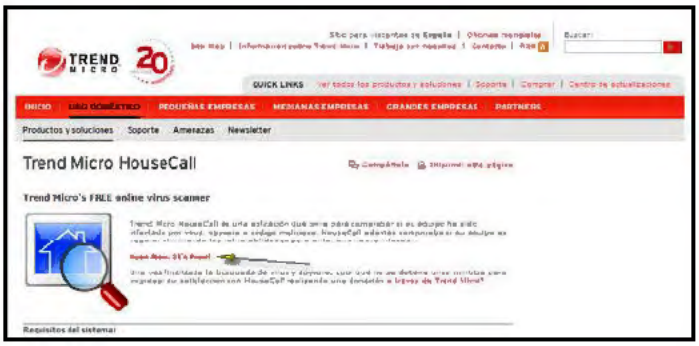
Para utilizar se va a la página web (http://www.pandasecurity.com/spain/homeusers/solutions/activescan/), se pulsa en "analiza tu PC". Entonces solicita instalar un complemento para el navegador para poder iniciarse, se siguen los pasos y aparece:

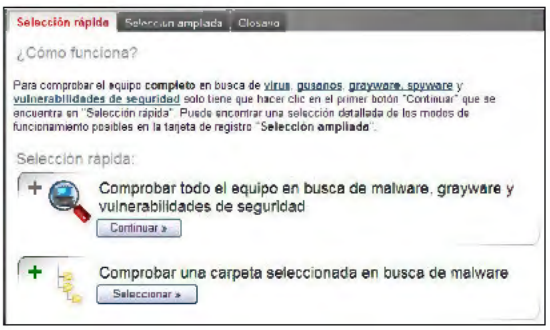
Se clica en "analizar", cuando ha finalizado el análisis, si el ordenador está infectado aparece una pantalla en la cual indica que ficheros maliciosos se borran con servicios de pago y cuáles no (los gratuitos requieren un registro gratuito previo).

Trend Micro House Call.

Se trata de una solución completa que puede realizar búsqueda de software malicioso, software molesto (publicidad no solicitada, barras de usuario en el navegador, etc.), vulnerabilidades, software espía y exploración de puertos.

Para poder utilizarlo se accede a la página web (http://housecall.trendmicro.com/es/) se pulsa en "Scan Now. It's Free", se inicializa el antivirus y da para elegir instalar un applet Java (para Firefox e Internet Explorer) o un complemento de Internet Explorer. En ambas opciones el sistema (o el navegador) pregunta para poder instalar estos subprogramas.





Una vez instalados, aparecen las diferentes opciones en las pestañas de selección rápida y selección ampliada:

Entonces se produce el análisis que tardara en función de la conexión que se tenga. Al finalizar muestra los ficheros infectados y la opción de borrarlos.

3.3 ANALIZADORES DE URL

Son programas que se instalan en el navegador y son capaces de categorizar las páginas que se desea visitar de modo que, atendiendo a esa valoración, se puede evitar que el sistema sea infectado por acceder a páginas peligrosas.

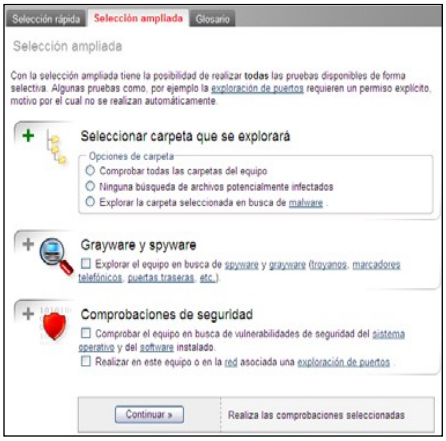
Estas herramientas pueden detectar, y a veces hasta bloquear, el acceso a páginas que contengan código malicioso, fraude electrónico, contenidos inapropiados e incluso si el código intenta explotar alguna vulnerabilidad sobre nuestro navegador o sistema.

No se asegura que la información que puedan ofrecer sea del todo fiable al 100%, bien porque la página Web solicitada no haya sido todavía analizada, o porque puedan existir opiniones distantes de diferentes internautas sobre un mismo sitio Web.

McAfee SiteAdvisor.

Las valoraciones que se realizan se basan en pruebas realizadas previamente sobre el sitio Web, y muestra información detallada sobre las descargas que se realizan desde la página, si contienen o no código malicioso, cataloga si los sitios con los que enlaza son o no seguros, contabiliza el número de correos electrónicos que se reciben en el caso de registrarse en alguno de sus servicios, determina si incluye ventanas emergentes de publicidad que puedan resultar molestas, e incluso si intenta explotar alguna vulnerabilidad de nuestro sistema

Instalación



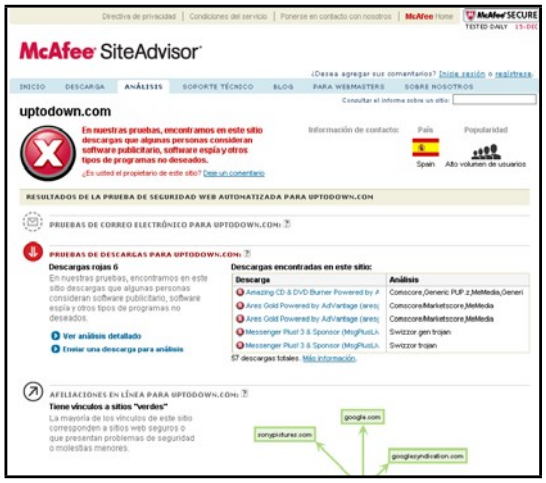
Desde la página del programa (http://www.siteadvisor.com) se hace clic en "Descargar ahora", la página detecta el navegador y ofrece descargar el programa específico:

- En Firefox 3: Se instala como cualquier otro complemento.
- En Internet Explorer 7: Se descarga un programa que cuando se ejecuta instala un complemento del navegador.

Uso Básico

El funcionamiento es muy sencillo, cuando se navega, mediante un sencillo código de colores muestra la valoración de la página:

También ofrece la opción de que aparezca este mismo código de colores en los principales buscadores (Google, Yahoo o Live Search).



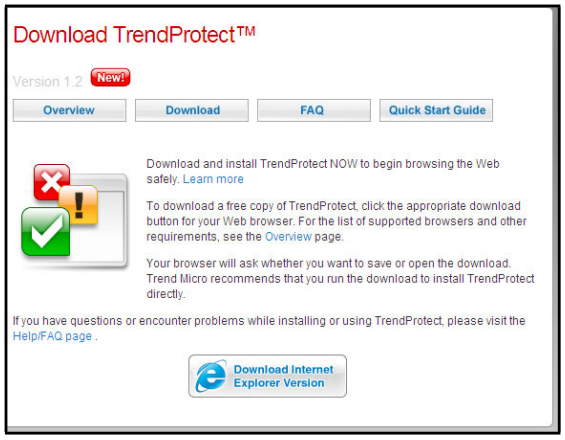
Estos iconos aparecen junto a los resultados del buscador,

ofreciendo una calificación (pagina segura, no segura o tenga cuidado)

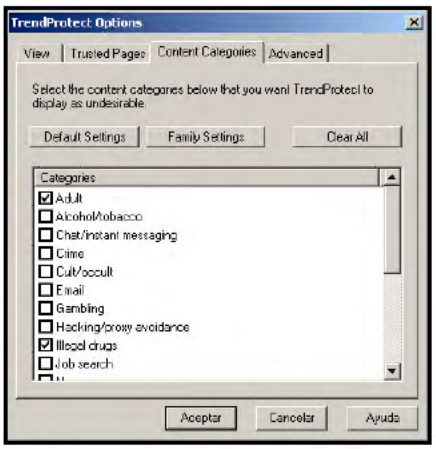
Además, entre las opciones que ofrece hay un completo informe del sitio en el que se está navegando con información sobre los ficheros que se pueden descargar de dicha pagina (si son sospechosos o no), la confiabilidad de los sitios a los que enlaza o si es un sitio Web con ventanas emergentes, entre otras opciones.

Trend Protect.

Es un complemento de Internet Explorer que se basa en las valoraciones realizadas por Trend Micro a través de servidores que rastrean las páginas y realizan clasificaciones de las mismas. Es una herramienta capaz de detectar si la pagina posee código malicioso e incluso si el contenido de esta es inapropiado.



Instalación



A través de la pagina web de Trend Micro se puede acceder a la herramienta (http://www.trendsecure.com/portal/en-US/tools/security_tools/trendprotect).

Se descarga y se instala como un complemento del navegador y aparece en la parte superior del navegador.

Uso Básico

Mediante un código de colores indica si la pagina en la que se está navegando es segura, no segura o sospechosa.

Además también indica si se trata de contenido inapropiado.

Contenido inapropiado.

La clasificación de dicho contenido puede modificarse a través de las opciones (botón derecho sobre el icono del programa).

Se encuentra integrado con los principales buscadores (Google, Yahoo y Live Search) para ofrecer iconos que indican la clasificación y destacando de los resultados del buscador.

Finjan SecureBrowsing.

Finjan SecureBrowsing

Analiza en tiempo real, con ayuda de los motores antivirus de Sophos y Kaspersky los resultados de los principales buscadores para determinar si las páginas que se muestran son o no seguras y pueden o no contener código malicioso.

Instalación

Desde la página del programa (http://www.finjan.com/Content.aspx?id=1460) se hace clic en el "Download" correspondiente:

- En Firefox 3: Se instala como cualquier otro complemento.
- En Internet Explorer 7: Se descarga un programa que cuando se ejecuta instala un complemento del navegador.

Uso Básico

Analiza los resultados de los buscadores (Yahoo, Google y Live Search), para mediante iconos indicar si es segura o no, o si no se ha podido analizar.

3.4 CORTAFUEGOS

Son programas que nos ayudan a controlar las conexiones que puede iniciar o recibir un ordenador conectado a la red. También nos protegen de intrusiones no deseadas, evita que la información sensible que se almacena en el ordenador pueda ser sustraída sin conocimiento del usuario. Un cortafuegos es como un guardia de seguridad que se mantiene vigilante a los ataques exteriores que intenten acceder al sistema y bloquea las comunicaciones hacia y desde fuentes no autorizadas.

Los cortafuegos personales, en general, están pensados para ser instalados en un PC doméstico conectado directamente a Internet. El control de las conexiones salientes es interesante para evitar que programas espías o troyanos puedan enviar información a Internet sin el consentimiento del usuario. El control de las conexiones entrantes sirve para impedir que los servicios del ordenador sean visibles en Internet, como la compartición de ficheros de Windows.

Además suelen descartar todo el tráfico no deseado, haciendo el PC invisible a barridos aleatorios de atacantes. También es habitual que incorporen un modo de aprendizaje, en el que preguntan al usuario cada vez que se inicia una conexión no reconocida si debe permitirse o no.

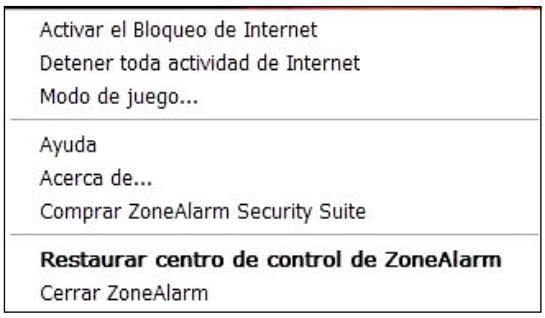
Algunos sistemas operativos incluyen un cortafuegos activado por defecto (como por ejemplo Windows XP y Vista), es recomendable que asegurarse que se encuentra activado en la computadora.

Si el sistema operativo de la computadora no incluye un cortafuegos, recomendamos que instalar uno. Hay que tener en cuenta que no es conveniente tener más de un cortafuegos ejecutándose simultáneamente en una misma máquina, por lo que si se desea utilizar el cortafuegos de Microsoft, no es necesario instalar ningún otro; y viceversa, si se desea usar otro cortafuegos es aconsejable desactivar el de Microsoft.

Zone Alarm.

ZoneAlarm permite bloquear tráfico no deseado y restringir el acceso no deseado de aplicaciones a Internet. Diferencia entre zona local y zona Internet a la hora de establecer restricciones de accesos. Por defecto, bloquea el acceso externo a todos los servicios del sistema permitiendo solamente el acceso a aquellos explícitamente indicados, por lo que al principio el programa hará más solicitudes para saber qué programas tienen acceso a la red. Permite un modo de juego para suprimir los análisis y actualizaciones para evitar interrupciones, bloquea sitios con programas espías y ayuda a detectar y recuperarse de robos de identidad. Por otro lado, determina si los programas del equipo pueden modificar la página de inicio de Internet Explorer

o instalar controles ActiveX. Cada vez que se produce una entrado o salida se realiza la pregunta para permitir o denegar el acceso de programa a la red. Se puede marcar la casilla para que el sistema siempre recuerde la acción de permitir o denegar el acceso.

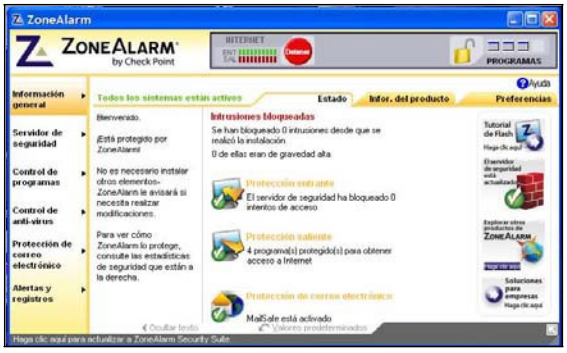


Instalación

El proceso de instalación es sencillo. Sólo hay que descargar el programa de la página oficial del producto a través de este enlace:

http://www.zonealarm.com/store/content/catalog/products/zonealarm_free_firewall_b.jsp?dc=34std&ctry=ES&lang=es.

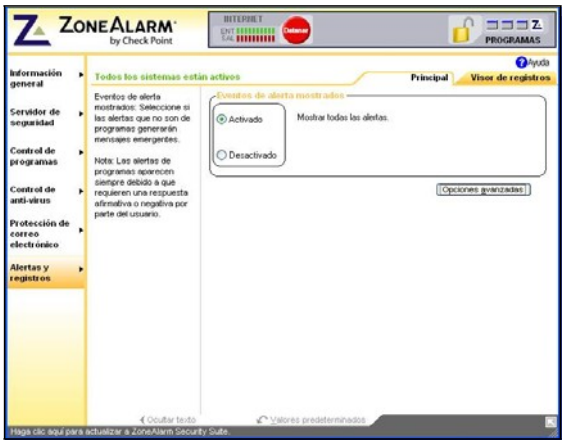
Una vez descargado el programa en el ordenador, se ejecute el archivo de instalación . El enlace de la página oficial no baja el programa, sino que ejecutando lo que hemos bajado de la pagina se baja el programa y se instala, una vez realizada la instalación, se reinicia el equipo.



En la primera ejecución del programa. Por defecto lo configuraremos automáticamente con los parámetros de la red, marcamos para ello la casilla correspondiente. Para finalizar pulsamos el botón ***Siguiente***.

Uso básico

En la fase inicial, desde que se instaló el producto. Tenemos que contestar al programa a un mayor número de preguntas, ya que a medida que se vaya produciendo el acceso de los diferentes programas a la red, no solicitará el permiso para programa. Ya que cada acción que desconozca el programa nos preguntará qué deseamos. Nos preguntará si queremos admitir la conexión del programa.



En el caso de que desconfiemos de una conexión podemos negar la conexión. Lo podemos hacer de manera temporal, o de manera definitiva marcando la opción de recordar lo que hemos seleccionado previamente. Si no estamos seguros sobre alguna petición de conexión, podemos consultar en foros especializados como INTECO-CERT.

Configuraremos el programa por defecto, para que nos realice una pregunta cada vez que se realiza una conexión desconocida. Así podremos monitorizar cada una de las conexiones que se va produciendo.

Para comprobar que el cortafuegos está activado, se debe de mostrar el icono en el “área de notificación”.

Comodo.

Es un cortafuegos que una vez instalado, por cada proceso en ejecución que se vaya a conectar a Internet, el cortafuegos muestra un mensaje de aviso, que permite interrumpir o no su ejecución; hay que autorizar la ejecución sólo de los procesos que sean de total confianza (procesos del sistema, procesos pertenecientes a aplicaciones instaladas en el sistema, etc.). Alguna de las opciones que presenta son: configurar el acceso a sitios Web, definir aplicaciones de confianza, restringir el acceso a páginas Web o aplicaciones SW, bloquear librerías en ejecución que se consideran posibles amenazas para el sistema, controlar el flujo de tráfico de Internet, definir reglas de filtrado, comprobar si el comportamiento de las conexiones es o no sospechoso, etc.

Instalación

El proceso de instalación es sencillo. Sólo hay que descargar el programa de la página oficial del producto a través del siguiente enlace:

http://www.personalfirewall.comodo.com/index.html

En uno de los pasos nos mostrará un aviso sobre el corte temporal de la conexión a Internet y un aviso de no apagar el equipo durante el proceso de instalación, no hay ningún problema. Marcamos sólo la opción de instalar el Cortafuegos (Install COMODO Firewall).

Configuramos el cortafuegos con defensa pro-activa óptima. Las opciones de “Firewall only” tiene controles menos estrictos y “Firewall with Maximum Proactive Defense +” tiene una seguridad más avanzada. Una vez marcadas pulsamos sobre el botón siguiente (Next).

Para no modificar las opciones de su navegador, desmarcamos todas las opciones que vienen marcadas por defecto. Seguidamente pulsamos sobre el botón siguiente (Next). La instalación puede llevar unos minutos

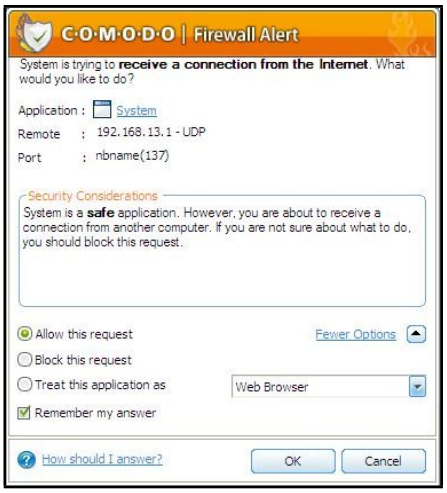
Una vez instalado el producto, dejamos marcado la casilla “Scan my system for malware” para que haga un chequeo de nuestro sistema. Pulsamos sobre el botón finalizar (Finish).

Después del reinicio obligatorio tras la instalación aparecerán probablemente las primeras ventanas de alerta.

Uso básico

El uso va dirigido a prevenir a los atacantes remotos no autorizados que pretenden obtener información privada.

Inicialmente, desde que se instaló el producto se harán preguntas sobre el permiso o denegación de que los programas puedan acceder a la red. Tenemos que contestar al programa a un mayor número de preguntas al principio, ya que cada acción que desconozca nos preguntará que deseamos hacer respecto a la entrada o salida de información de nuestro ordenador. Nos preguntará si queremos admitir la conexión de un programa hacia fuera o hacia dentro.



Podemos recordar nuestra contestación marcando la casilla “Remember my answer”, así cada vez que vuelva a suceder un evento de las mismas características, actuará en relación a la contestación anterior.

En el apartado de defensa (Defense+) puede ver todos los programas bloqueados, los sucesos que se han producido, para analizar lo que está sucediendo en su ordenador.

Dentro del apartado de Firewall, se pueden configurar todas la características del cortafuegos, definiendo manualmente las aplicaciones y zonas de confianza. Además podemos visualizar información relativa a la configuración del cortafuegos.

En nuestra área de notificación, podemos ver que el cortafuegos esté activado, cuando se muestra el icono cómo el indicado en la figura.

Ashampoo.

Ashampoo Firewall es un cortafuegos que posee una interfaz auto-explicativa. En el modo experto se pueden crear reglas para cada programa indicando el puerto y el tipo de conexión utilizados. Permite monitorizar conexiones de área local y las internas del ordenador así como las externas, actualizándose continuamente. Es posible además, mantener un registro de las conexiones internas, LAN y de Internet de forma detallada (hora, fecha, aplicación, puerto y dirección IP). También muestra todos los procesos activos en el sistema. Dispone de un modo de auto aprendizaje para identificar los programas que intentan conectarse y decidir si permitirlo o no. Por último, como utilidad interesante, cabe destacar la opción 'Bloquear todo' que permite detener la totalidad del tráfico existente.

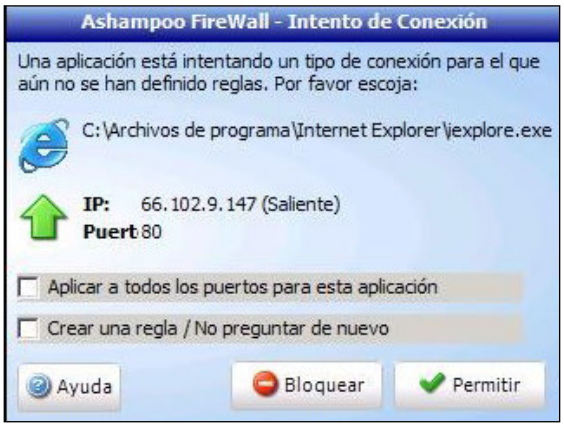
Necesita registro para obtener la clave gratuita para el funcionamiento del programa. Sólo es necesario introducir una dirección de correo válida.

Instalación

Descargar la aplicación de sitio oficial del producto, y ejecutar el archivo descargado:

http://www2.ashampoo.com/webcache/html/1/product_11_0050_.htm

Seleccionamos el idioma para el producto. Seguidamente pulsamos sobre el botón OK. La instalación puede tardar unos minutos. Una vez finalizada la instalación, se requiere la reinicialización del ordenador. Marcamos el reinicio (Yes, restart the computer now) y pulsamos sobre el botón finalizar (Finish).



Uso básico

La herramienta tiene varios métodos de protección. La más normal es en la que se monitoriza el tráfico entrante y saliente, y se pregunta al usuario si desea admitir la conexión de entrada o salida. No protege así de todas las actividades de red y le protege tanto contra las conexiones entrantes como salientes.

También podemos crear reglas para los programas o controlar el acceso a la red. Y dispone de una opción de emergencia para bloquear todo el tráfico, ante un ataque o un programa malicioso activo.

En la pantalla se muestran el aviso que nos da el programa cuando algún programa intenta realizar una conexión. Nos muestra información sobre el tipo de programa que desea realizar la conexión. En el caso de que esta respuesta sea permanente, marcar la opción de crear una regla.

3.5 CONTROL PARENTAL

Las herramientas de control parental utilizan y combinan diferentes técnicas para el filtrado y monitorización de contenidos de internet que son inapropiados para determinadas edades (pornografía, drogas...) e incluso reprobables (violencia, racismo, xenofobia...). Los métodos empleados y la facilidad de optimización por parte del usuario pueden variar mucho entre ellas.

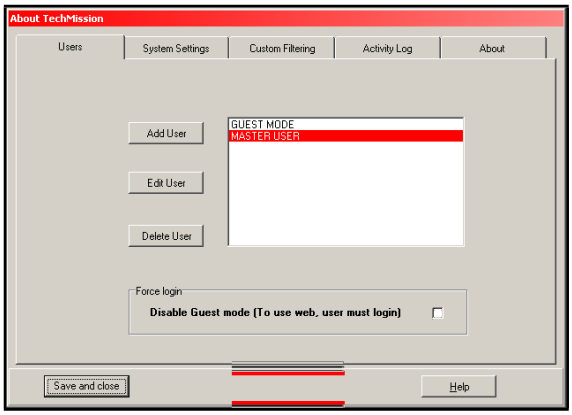
Antes de instalar una solución de control parental se recomienda consultar al proveedor de servicios de Internet (ISP). Muchos de ellos ofrecen como servicio a sus usuarios por una pequeña cuota sistemas de filtrado en sus redes similares a los aquí descritos.

Hay que tener en cuenta que estas herramientas no son soluciones efectivas al 100% y que no están para sustituir la supervisión que deben realizar padres y educadores.

TechMission.

TechMission es una herramienta de control parental que utiliza filtrado por palabras clave y mediante un sistema de listas blancas y negras de enlaces que se pueden administrar.

Se pueden crear varios usuarios diferentes en función de la edad y del nivel de restricción que se le quiera dar a cada uno de ellos. Dispone de hasta ocho niveles de restricción de contenidos, tales como pornografía, drogas, violencia, racismo, etc.



Instalación

Desde la siguiente página web (http://www.safefamilies.org/downloadstep.php) se puede descargar pulsando sobre el enlace Downloads.

La instalación se realiza por medio de un asistente que automatiza la misma. Una vez instalada, pide una contraseña para el acceso del usuario de administración del programa.

Desde la consola de administración del programa se pueden crear diferentes perfiles de usuario, pudiendo personalizar para cada uno de ellos unas restricciones diferentes. Estos perfiles están protegidos por contraseña.

Pulsando con el botón derecho del ratón sobre el icono situado en la barra de tareas de Windows se puede cambiar de usuario.

Uso Básico

Al iniciar el sistema, la herramienta se ejecuta cargando las restricciones del usuario que se haya cargado en la sesión anterior.

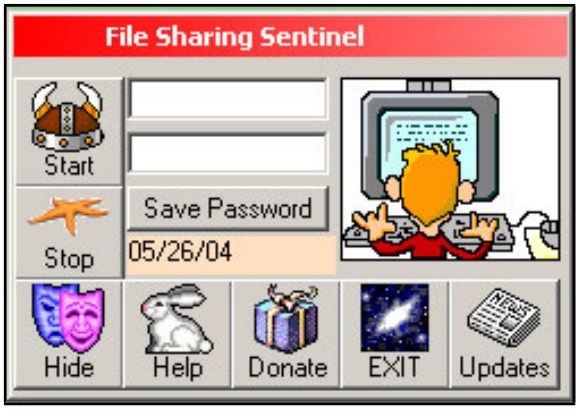
Pulsando con el botón derecho del ratón sobre el icono situado en la barra de tareas de Windows se puede cambiar este usuario.

La herramienta bloquea todos los contenidos que estén dentro de las restricciones impuestas al usuario.

File Sharing Sentinel.

File Sharing Sentinel es una herramienta de control parental diseñada para bloquear el uso compartido de archivos P2P. También dispone de función anti-spyware, impidiendo la instalación de programas espía en el sistema del usuario.

Está especialmente diseñado para evitar la descarga por parte de menores de ficheros con contenido inadecuado (pornográfico) o malicioso (virus).



Instalación

Desde la siguiente página web (http://www.akidthaine.com) se puede descargar pulsando sobre el enlace Downloads.

La instalación se realiza por medio de un asistente que automatiza la misma. Una vez instalada, pide una contraseña para el acceso a la consola de administración del programa.

Uso Básico

La herramienta viene pre configurada y las únicas acciones que se pueden realizar desde la consola de administración son la de activar el escaneo (botón Start) o la de pararlo (botón Stop).

Una vez que está activada, bloquea los intentos de instalación de nuevas aplicaciones de tipo P2P y las descargas de estas.

K9 Web Protection.

K9 Web Protection es un filtro de contenidos por categorías altamente configurable que funciona como servicio Web.

Las páginas solicitadas por el navegador son antes categorizadas en sus servidores mediante tecnologías de filtrado basadas en análisis estadísticos e inteligencia

artificial para comprobar que se ajustan a nuestras preferencias. Permite restricciones por tiempo, listas blancas y negras, además de control sobre aplicaciones P2P, salas de Chat y mensajería instantánea. También es útil para monitorizar la actividad en Internet.

Instalación

Desde la siguiente página web (http://www1.k9webprotection.com/getk9/index.php) se puede iniciar la descarga del programa tras rellenar un pequeño formulario con nuestro nombre y correo electrónico de contacto donde nos remitirán una clave de licencia necesaria durante la instalación.

La instalación se realiza siguiendo las instrucciones enviadas al correo electrónico. En dichas instrucciones se proporciona un enlace de descarga de la herramienta. Una vez instalada, pide una contraseña para el acceso a la consola de administración del programa.

Uso Básico

La tecnología de filtrado utilizada divide el contenido de Internet en más de 55 categorías distintas. Podemos usar la configuración por defecto, o mediante el panel de administración al que accedemos vía Web gestionar nuestras preferencias indicando que categorías queremos bloquear y cuáles no.

Hay multitud de posibilidades, desde escoger una de las configuraciones ya establecidas hasta personalizar una por una. El filtro posee una gran flexibilidad, dispone de categorías tan variadas que van desde "Education Sex" (Educación Sexual) hasta "Spyware/Malware Sources" (Fuentes Spyware/Malware), que según comentan en su Web ayuda a reducir drásticamente las probabilidades de infección.

A esto hay que sumarle que desde el mismo panel de administración tenemos la posibilidad de bloquear aplicaciones P2P, salas de Chat, mensajería instantánea y páginas de navegación anónima; incluir listas blancas y negras, activar Google SafeSearch, establecer restricciones de tiempo y bloquear URL por palabra clave.

El panel de administración está protegido por contraseña para que no pueda deshabilitarse por usuarios desautorizados. Con esa misma contraseña podemos habilitar temporalmente páginas bloqueadas en caso de querer acceder a ellas.

También dispone de una sección para monitorizar la actividad de Internet, con informes detallados sobre las páginas solicitadas y bloqueadas.

Como apunte decir que K9 Web Protection al funcionar como servicio web recopila cierto tipo de información como IP y páginas solicitadas. Esto afecta a la privacidad de los usuarios por lo que se recomienda antes de utilizar su servicio estar de acuerdo con la política de privacidad de Blue Coat.

3.6 ANTIESPIAS.

Los *Spywares* o Programas Espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas sin el consentimiento del usuario del mismo, para luego ser enviada a través de Internet a un destinatario, generalmente a alguna empresa de publicidad. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar terceros programas, por lo que rara vez el usuario es consciente de ello.

A-squared Free.

A-squared Free escanea el sistema en busca de programas espías y otro tipo de código malicioso como troyanos, gusanos o dialers. Permite la selección de las unidades de disco, directorios o ficheros individuales a analizar.

Dispone de diversas opciones de análisis: escaneo de registro, memoria, búsqueda de código potencialmente peligroso y uso de heurística.

Permite la eliminación de ficheros infectados y almacena informes de uso en formato HTML. Dispone de actualización en línea a petición del usuario y se puede instalar en los sistemas operativos Windows 98, ME, 2000, 2000 Server, XP y 2003 Server.

Instalación

Desde la página web de la aplicación (http://www.emsisoft.es/es/software/download) se puede descargar pulsando sobre el botón Download.

La instalación se realiza por medio de un instalador que lanza un sencillo asistente que automatiza la instalación.

Uso Básico

El funcionamiento es sencillo e intuitivo. Para escanear el equipo en busca de programas espías sólo hay que seleccionar la pestaña Examinar ordenador para elegir entre las diferentes modalidades de escaneo disponibles (rápido, inteligente, a fondo o personalizado).

Una vez realizado el escaneo muestra un resumen de las incidencias encontradas, pudiendo eliminar o poner en cuarentena los programas detectados.

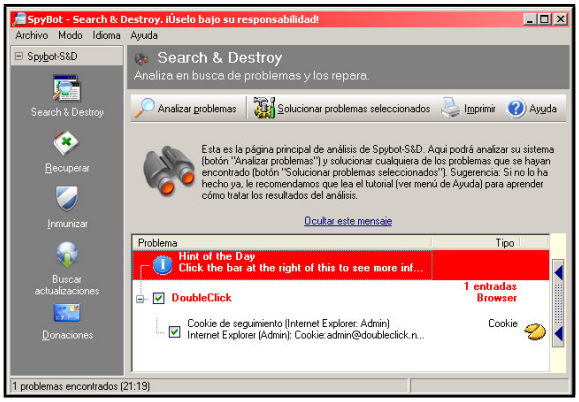
Spybot S&D.

Spybot S&D es una sencilla aplicación para detectar y eliminar programas espía, que puede dejarse residente en la memoria del sistema del usuario para que avise cada vez que se intente escribir en el registro de Windows

Tiene capacidad de eliminación de los programas espía encontrados, así como de evitar el secuestro del navegador; para lo cual hay que activar la opción de Modo Avanzado

configurándola desde la pestaña Herramientas marcando la opción de Páginas del navegador.

Se puede instalar en los Sistemas Operativos Windows a partir de Windows 98.



Instalación

Desde la página web de la aplicación (http://www.spybot.info/es/download/index.html) se puede descargar pulsando sobre el botón Download.

La instalación se realiza por medio de un instalador que lanza un sencillo asistente que automatiza la instalación.

Uso Básico

El funcionamiento es sencillo e intuitivo. Para escanear el equipo en busca de programas espías únicamente hay que pulsar el botón Analizar problemas desde la pestaña Search & Destroy para que la aplicación comience a funcionar.

Ad-Aware 2008 Free.

Ad-Aware 2008 Free es la versión gratuita, limitada y de uso particular de la herramienta comercial que distribuye Lavasoft, la cual escanea el sistema del usuario en busca de programas espía.

Tiene capacidad de eliminación de los programas espía encontrados, y se puede actualizar a través de Internet. También te permite eliminar el contenido de la cache, cookies, historial, etc. de los navegadores Internet Explorer, Firefox y Opera.

Instalación

Desde la página web de la aplicación (http://www.adaware.es/fiche.html?REF=658638) se puede descargar pulsando sobre el botón Probar gratis.

La instalación se realiza por medio de un instalador que lanza un sencillo asistente que automatiza la instalación.

Uso Básico

Para escanear el sistema en busca de programas espía únicamente hay que pulsar el botón Explorar tras seleccionar el modo de exploración más adecuado a las necesidades del usuario. Se puede optar por una

exploración inteligente, completa o personalizada.

Una vez escaneado el sistema se puede optar por eliminar el programa espía o mantenerlo en cuarentena.

3.7 Servicios de seguridad ofrecidos por los principales ISP(1).

	Anti-Virus	Antispyware	Antiphishing	Antispam	Firewall	Antispam	Asistencia	Sustitución de equipo	Puesta a punto	Control parental
Orange	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Telefónica	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Vodafone	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Ono	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗

(1) Proveedores de servicios de Internet

4. HERRAMIENTAS DE PAGO

En este apartado ofrecemos una lista exhaustiva de las soluciones de pago existentes en el mercado, para los diferentes tipo de herramientas.

	Anti-Virus	Cortafuegos	Antiespías	Protección web	Protecc. de correo electrónico	Suite de seguridad	Control parental
AhnLab (V3)	✓	✗	✓	✓	✓	✓	✗
ALWIL (Avast! Antivirus)	✓	✗	✓	✓	✓	✓	✗
Authentium (Command Antivirus)	✓	✓	✓	✓	✓	✓	✓
AVG Technologies (AVG)	✓	✓	✓	✓	✓	✓	✗
Avira (AntiVir)	✓	✓	✓	✓	✓	✓	✗
BitDefender GmbH. (BitDefender)	✓	✓	✓	✓	✓	✓	✓
Cat Computer Services (Quick Heal)	✓	✓	✓	✓	✓	✓	✗
Eset Software (ESET NOD32)	✓	✓	✓	✓	✓	✓	✗
FRISK Software (F-Prot)	✓	✓	✓	✓	✓	✓	✗
F-Secure (F-Secure)	✓	✓	✓	✓	✗	✓	✗
G DATA Software (GData)	✓	✓	✓	✓	✓	✓	✓
Hacksoft (The Hacker)	✓	✓	✓	✓	✓	✓	✗
Hauri (ViRobot)	✓	✓	✓	✓	✓	✓	✗
K7 Computing (K7AntiVirus)	✓	✓	✓	✓	✓	✓	✗
Kaspersky Lab (AVP)	✓	✓	✓	✓	✓	✓	✓
McAfee (VirusScan)	✓	✓	✓	✓	✓	✓	✓
Microsoft (Malware Protection)	✓	✓	✓	✓	✓	✓	✗
Norman (Norman Antivirus)	✓	✓	✓	✓	✓	✓	✓
Panda Security (Panda Platinum)	✓	✓	✓	✓	✓	✓	✓
PC Tools (PCTools)	✓	✓	✓	✓	✓	✓	✗
Prevx (Prevx1)	✓	✓	✓	✓	✓	✓	✗
Rising Antivirus (Rising)	✓	✓	✓	✓	✓	✓	✗
Sunbelt Software (Antivirus)	✓	✓	✓	✓	✓	✓	✗
Symantec (Norton Antivirus)	✓	✓	✓	✓	✓	✓	✓
VirusBlokAda (VBA32)	✓	✗	✓	✓	✓	✓	✗
Trend Micro (TrendMicro)	✓	✓	✓	✓	✓	✓	✓
VirusBuster (VirusBuster)	✓	✓	✓	✓	✓	✓	✗
MySecurityCenter	✓	✓	✓	✓	✓	✓	✓