



Internet Aula Abierta 2.0.

Seguridad Informática

Índice

Seguridad.....	1
Normas básicas.....	2
Seguridad del ordenador.....	3
Consejos para utilizar internet.....	6
Antivirus y otras utilidades.....	9
Cortafuegos.....	12
Conceptos generales.....	13
Firewall de Windows 7.....	16
ZoneAlarm.....	21
Spyware.....	27
¿Qué es?.....	28
Windows Defender.....	29
Ad-Aware.....	34
Windows Update.....	39
Actualización en Windows XP.....	40
Actualización en Windows 7.....	43
Publicar en Internet.....	49
Actividades.....	53

Seguridad

Cuando estamos conectados a Internet tenemos que saber que estamos comunicándonos con otros ordenadores de la Red, es decir, estamos abriendo nuestro ordenador al exterior. Esa puerta que abrimos al exterior nos permite estar en contacto con todo un mundo lleno de posibilidades, pero también posibilita que intrusos puedan acceder a nuestro ordenador y poner en riesgo nuestros datos.

Sin unas mínimas medidas de seguridad somos muy vulnerables y podremos poner en riesgo toda nuestra información.

En este bloque temático te indicamos una serie de normas básicas de seguridad, programas y consejos que te ayudarán a proteger tu ordenador y navegar por Internet de un modo más seguro.



Normas básicas

La utilización de herramientas tecnológicas exige, al igual que ocurre con cualquier otro tipo de herramientas, comportarse de forma prudente para evitar consecuencias negativas. Antes de continuar queremos subrayar que la prudencia no tiene nada que ver con la paranoia: es una actitud vigilante pero tranquila que salvaguarda nuestra seguridad y nuestros intereses.

Adoptando pues esta actitud básica podemos decir que existen conductas de protección de la seguridad de tipo activo y de tipo pasivo. Sería algo similar a lo que ocurre cuando nos ponemos al volante de un coche: abrocharse el cinturón supone dotarnos de una protección pasiva, mientras que mantener una velocidad adecuada o regular las paradas para que el cansancio no nos provoque sueño entraría dentro de conductas activas que, en ambos casos, redundan en un aumento de la seguridad.



Seguridad del ordenador

Dentro de las conductas que hemos denominado pasivas podríamos destacar las siguientes:

- Configurar nuestro sistema operativo para que obtenga e instale de forma automática las actualizaciones y parches de seguridad que sean necesarios.
- Obtener e instalar un antivirus que disponga de actualización automática y configurarlo de forma que revise, también de forma automática, el correo, los archivos descargados y, en general, cualquier archivo que podamos abrir en nuestro ordenador.
- Proteger nuestro equipo del acceso no autorizado del exterior, así como evitar la salida inadvertida de datos desde el mismo, instalando y configurando un cortafuegos, especialmente si disponemos de una conexión constante a Internet.
- Apagar aquellos equipos que tengan posibilidad de acceder de forma constante a Internet cuando no se utilicen.
- Si eres usuario de Windows es probable que la utilización de contraseñas para acceder al sistema te resulte un procedimiento poco habitual y que lo consideres incómodo. No estaría de más que te plantearas la creación de un perfil de usuario con permisos limitados, dejando los permisos de administrador sólo para aquellos momentos en los que tuvieras que instalar algún programa. Lógicamente la misma recomendación es válida para sistemas Linux, aunque en este caso lo habitual es hacerlo. Si no lo haces así es posible que algún código malicioso se aproveche de tu acceso libre con permisos absolutos para instalar virus, gusanos, troyanos y otros especímenes.



Comprobando la seguridad


En esta ocasión vamos a empezar realizando una práctica que te permitirá comprobar el grado de seguridad de tu equipo.



Práctica

Conéctate a la dirección <http://www.internautas.org/w-scanonline.php>

Comprueba los resultados. Si aparece todo en verde, tu equipo está protegido.

 **INVISIBLE** y el colofón de la información es el mensaje anterior, quiere decir que tu equipo está protegido contra las intrusiones desde el exterior y es probable que hayas puesto en práctica la mayoría de las medidas que se van a comentar en este módulo. En caso contrario necesitarás mejorar la seguridad de tu sistema para lo cual tendrás que modificar algunas conductas en tu navegación por la red y dotarte de algunas herramientas que te ayuden a protegerte de accesos indeseados.



Práctica

Si quieres corroborar los resultados anteriores puedes conectarte a grc.com/default.htm, localiza el enlace **ShieldsUP!** y pulsa sobre él.

Pulsa ahora el botón **Proceed**  que te llevará a una nueva página en la que podrás escoger los servicios que quieres escanear. Lo más recomendable es que selecciones  para hacer un test completo a todos los puertos.

En esta ocasión el objetivo es que la matriz que representa los 1056 primeros puertos (del 0 al 1055) tenga todos los cuadritos en verde (puertos invisibles) y no presente ningún cuadradito rojo pues ese color indicaría que lo tenemos puertos abiertos que pueden ser usados para acceder a nuestro sistema.

0		31
32		63
64		95
96		127
128		159
160		191
192		223
224		255
256		287
288		319
320		351
352		383
384		415
416		447
448		479
480		511
512		543
544		575
576		607
608		639
640		671
672		703
704		735
736		767
768		799
800		831
832		863
864		895
896		927
928		959
960		991
992		1023
1024		1055

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

■ Open
 ■ Closed
 ■ Stealth

Total elapsed testing time: 68.205 seconds


[Text Summary](#)

Consejos para utilizar Internet

Te damos algunos consejos que deberían convertirse en pautas activas de conducta cuando utilices Internet:

- **Actualiza regularmente el software** de tu ordenador a las versiones más recientes.
- **Realiza copias de seguridad** de tus datos cada cierto tiempo. Reinstalar un sistema operativo con todas sus aplicaciones puede ser muy pesado, pero es algo casi mecánico,...rehacer dos años de trabajo suele ser imposible.
- Si accedes a Internet mediante un módem-router **revisa** de vez en cuando el Acceso Telefónico a Redes para ver la **conexión, los filtros y contraseña**.
- Cuando accedas en Internet a **sitios identificados desde ordenadores públicos o compartidos**, acuérdate de **salir** de dichos sitios **cerrando la sesión y el navegador** para que no quede activa tu identidad.
- Ten **cuidado con algunas páginas**, sobre todo las de juegos, contenido para adultos y algunas de descargas gratuitas, que te piden que instales programas para optimizar el acceso: en la mayoría de los casos se trata de métodos para instalar programas de control de tu ordenador.



- Si tienes que introducir información sensible, como por ejemplo el número de tu tarjeta de crédito, en una página web, no lo hagas nunca si no se trata de una **conexión segura**: en el campo de protocolo de la dirección pondrá **https**: en lugar de **http**: y en tu barra de estado o en la misma barra de dirección aparecerá el símbolo .
- Si necesitas realizar compras o pagos por Internet la mayoría de los bancos suelen tener una **tarjeta virtual de crédito** con coordenadas que garantiza la seguridad de las compras.
- **No te fíes de los enlaces de las páginas** que te llegan por correos o medios desconocidos, especialmente cuando accedas a páginas de servicios bancarios o de comercio electrónico. Comprueba que te conducen donde realmente quieras ir.
- **Configura tu cliente de correo** con los filtros y métodos de seguridad que posea. Un

sistema puede ser configurarlo para recibir y enviar en modo texto, tal vez quede algo más soso, pero evitaras una fuente de problemas de seguridad y de privacidad.

- **Comprueba la extensión de los archivos que recibes** por correo electrónico. No los abras nunca si se trata de ejecutables o de precedencia dudosa o desconocida.
- Tus amigos, esos que no saben decir en inglés más que "yes", no se han apuntado a una academia milagrosa y por eso te escriben ya en la lengua de Shakespeare: o bien tienen un virus en su ordenador o bien alguien ha usurpado su dirección, pero lo que es seguro es que el **archivo adjunto que te envían es un código malicioso**.
- **Ni los bancos, ni ninguna otro servicio web** que necesite identificación, se va a poner en contacto contigo por correo electrónico para solicitar que **confirmes tu nombre de usuario y tu contraseña** desde un formulario en el propio mensaje de correo o desde una página a la que se te enlaza desde el mismo: se trata de una práctica para apoderarse de esos datos.
- **Cuando envíes archivos adjuntos coméntalo en el cuerpo del mensaje** y haz un breve resumen de su contenido. No envíes nunca archivos ejecutables.
- **Lee** despacio y con todo detalle todas **las ventanas que se muestran durante la instalación de cualquier aplicación** que descargues de Internet, incluso la licencia o el contrato del usuario final. De esta forma te aseguras de que no incluyen ningún software sospechoso.
- **Analiza periódicamente tu equipo con algún programa antiespía.**
- **No propagues bulos.** Cuando te llega un mensaje avisando de un peligro muy grave, cuando se hace tal o cual cosa, suele ser un bulo difundido por un amigo que te quiere bien pero no se ha preocupado de comprobar la veracidad del contenido. Muchas veces basta con hacer una lectura medianamente atenta y una simple búsqueda en Google para comprobar que el mensaje no es más que un bulo infundado.
- Cuando envíes mensajes grupales **acuérdate que existe la opción CCO o BCC** que permite en envío de direcciones ocultas (sobre todo si los destinatarios se desconocen entre ellos) pues si hacemos públicas las direcciones de correo electrónico es fácil que caigan en manos desconocidas y con propósitos muy diversos.
- No estaría de más que, de vez en cuando pasaras por alguna de las páginas que disponen de secciones divulgativas **sobre seguridad** para mantener tu información actualizada: [La Asociación de Usuarios de Internet](#), [Hispacec](#) o [El Instituto Nacional de Tecnologías de la Comunicación \(INTECO\)](#) pueden ser unos buenos puntos de referencia.
- Ten en cuenta los temas de **protección al menor**:
 1. Se debe concienciar al alumnado en un **uso adecuado de las redes sociales**.
 2. **No deben dar datos sensibles** (dirección, teléfono, fechas...) ni publicar material fotográfico o audiovisual que les pueda comprometer o ser utilizado de forma perniciosa.
 3. Tienen que **aprender a utilizar los chat y video-chat con seguridad**. Internet favorece el anonimato y la suplantación de identidad, así que los desconocidos no siempre son las personas que dicen ser.

4. La **comunicación a los padres o tutores de cualquier acoso**, vejación, proposición indecente,... es fundamental para poder solucionar los conflictos.
5. Los **docentes y padres pueden encontrar soluciones y programas** de protección en los siguientes enlaces:
 - **INTECO-Cert: Menores protegidos**: en este sitio se podrán encontrar consejos y recursos tanto para padres y educadores como para menores, programas e información sobre control parental para permitir el acceso a listas blancas y bloquear a listas negras, etc.
 - **Softonic**: uno de los múltiples sitios de descargas de software donde podrás buscar programas de control parental gratuitos y en español.
6. En el **ámbito familiar puede resultar más fácil la seguridad**, poniendo todos los medios posibles:
 - Conseguir un buen **clima de comunicación entre padres e hijos**,
 - **Supervisar el ordenador de nuestro hijo o hija**, como se supervisan las tareas de clase.
 - **Ubicar el ordenador en un espacio común**, abierto, no en una habitación cerrada sólo para nuestro hijo o hija.
 - Poner los medios de protección mediante los **ajustes de control de contenidos del navegador**,
 - **Instalar programas de seguridad como Netnanny, SafeFamilies, Optenet, Cyberpatrol**, etc. o,
 - Activar el propio **programa de control parental** del sistema operativo si se utiliza **Windows 7**.

Para finalizar dos últimos consejos:

- **Utiliza el sentido común**: no hagas en la red aquello que no harías en la vida real.
- Sigue el espíritu básico de la red y **ayuda a los demás dando a conocer las normas de seguridad**.

Los Virus

Los virus informáticos son programas malintencionados (malware) que se propagan entre los ordenadores sin el consentimiento de los propios usuarios y que tienen una intencionalidad oscura y generalmente dañina: tomar el control del equipo infectado, destrucción de datos, etc.

Este contagio y propagación de los virus se realiza por cualquier medio por el que se pueda comunicar nuestro ordenador con el exterior: Internet, unidades de almacenamiento externo, dispositivos USB, etc.

Algunas personas piensan que en el tema de los virus sólo corren riesgo de contagio cuando están conectados a Internet y no toman medidas respecto a otros ficheros que copian a su ordenador desde otras unidades o memorias USB. Siempre que hay comunicación y transferencia de datos hay posibilidad de contagio. No por no tener conexión a Internet estás a salvo de infecciones de malware, así que las medidas preventivas son una necesidad que debes solventar si quieres dar seguridad a los datos e información que posees en tu ordenador.

La denominación coloquial de virus se debe a la similitud con las características de los virus biológicos: propagación, contagio, vacuna, eliminación,... El término común engloba a una gran cantidad de programas informáticos hostiles e intrusivos de diferente tipo: troyanos, falsos o hoax, gusanos, etc.

El antídoto informático para este tipo de programa lo constituyen los antivirus, que al igual que las vacunas biológicas, su objetivo es detener los ataques de los virus y mantener en buena salud tu ordenador. Los antivirus pretenden dar seguridad en la transferencia de datos a los equipos informáticos, por eso intentan contrarrestar los ataques de programas malware anticipándose a ellos, bloqueando su acceso y eliminándolos.

La actualización continua de estos programas antivirus es tan necesaria como su existencia, pues de una permanente puesta al día depende la efectividad plena de su tarea.

Si no dispones aún de un antivirus actualizado tienes la posibilidad de aplicar algunas utilidades que se ofrecen de forma gratuita en la red, mediante las cuales podrás informarte de las últimas amenazas, realizar un análisis de tu equipo y descargar utilidades de desinfección en caso de que localices algún código maligno. Las tres que se muestran a continuación son ofrecidas gratuitamente por [Panda Software](#)

Chequeo on-line

Pulsa sobre la imagen para acceder al chequeo on-line de virus. Necesitarás una conexión activa para poder utilizarlo.

Panda ThreatWatch

Pulsa sobre la imagen para acceder a Panda ThreatWatch con las alertas de virus. Si tu conexión no está activa sólo verás este párrafo



Otros antivirus con servicio de chequeo on-line gratuito:

Cuando accedas a estos servicios deberás comprobar la cobertura que realizan para ver si se adaptan a tus necesidades:



Chequeo gratis de archivos on-line:



Algunos antivirus gratuitos para uso personal:

Algunos de los antivirus que te presentamos tienen la condición de un uso personal o un Windows original (caso de Microsoft Security Essentials), deberás ver las condiciones de uso antes de realizar la instalación.



Debes entender que es muy distinta una actualización de una instalación. Las actualizaciones son de un mismo programa, se suelen realizar de forma automática y generalmente no conllevan problemas en nuestro ordenador, pero la instalación de otro antivirus distinto del que tenemos, al tener los mismos objetivos, puede hacer que choque con el que tenemos ya instalado y alterarnos la configuración.

Para evitar problemas NO debes de instalar un antivirus si ya tienes instalado antes otro distinto. Lo recomendable es realizar una desinstalación previa del antivirus que tenemos y después instalar el nuevo. Para los chequeos on-line este requisito no es necesario.



Actividad 1

Localiza en la página de alguna empresa antivirus la "ficha técnica" de cuatro virus informáticos recientes, especificando su nombre, daño potencial, manera de manifestarse y propagarse. Averigua también a qué nos referimos cuando se habla de "phishing" y la forma de protegerte de este tipo de ataque.

Cortafuegos

Con la denominación cortafuegos (firewall) nos referimos a los programas que se encargan de monitorizar las transferencias de información que se producen desde y hacia nuestro ordenador.

En muchos casos estas transferencias de información corresponden a procesos que hemos iniciado voluntariamente y sus correspondientes respuestas, tales como peticiones de páginas web, envíos o recepciones de correo, exploración de las máquinas de nuestra red, consulta automática de actualizaciones de programas, etc. Pero también puede haber ocasiones en las que dichas transferencias se producen sin nuestra autorización y con finalidades que nada tienen que ver con nuestros intereses pudiendo, incluso, resultar particularmente perjudiciales.



Cortafuegos (firewall)

La red está plagada de aplicaciones y funcionalidades útiles e interesantes, aunque como en cualquier otro ámbito de las interacciones humanas existen personas o grupos malintencionados que diseñan aplicaciones perjudiciales. Ser prudente y mantener una adecuada preocupación por la seguridad es muy positivo; la actitud paranoica que nos lleve a sentir una constante amenaza será, como en cualquier otro ámbito, una patología que no reportará ningún beneficio.

Se hace imprescindible llevar un control de las comunicaciones que se producen a través de nuestra máquina para evitar que programas malintencionados nos espíen, utilicen nuestro ordenador para enmascararse o, simplemente se difundan desde nuestro equipo a través de las redes a las que estemos conectados. Lógicamente, cuanto más amplia sea nuestra conectividad, más importante es contar con alguna utilidad que controle el intercambio de información.



Para los usuarios de Windows anteriores a la versión de Windows XP (SP2), la carencia de una protección en el propio sistema operativo obligaba a la instalación de un programa cortafuegos complementario. Desde que Microsoft instaló en Windows XP (Service Pack2) y posteriores la opción de firewall activada por defecto, este tipo de programas de otras empresas ha dejado de tener la pujanza que tenían anteriormente.

Si nunca antes habías utilizado un cortafuegos es probable que te sientas algo desconcertado cuando te conectas a Internet y el programa empieza a preguntarte qué debe hacer en determinadas situaciones.

Para evitarlo veamos cuál es el **esquema básico de funcionamiento de un cortafuegos**:

1. Una aplicación intenta acceder a Internet.
2. Firewall comprueba si se encuentra dentro de las aplicaciones reconocidas.
 - A. Es una aplicación conocida y tiene adjudicadas unas reglas predefinidas. El programa aplica las reglas y permite o bloquea la conexión en función de lo establecido en ellas.
 - B. Es una aplicación desconocida o las condiciones de las reglas definidas no contemplan la situación actual. El programa nos pide que le indiquemos una acción a tomar, que puede depender de las posibilidades del programa o de la configuración establecida en él. Así se podría:
 1. Permitir o bloquear de forma continua esa aplicación.

2. Permitir o bloquear el acceso en esta ocasión.
 3. Utilizar alguna de las reglas correspondiente a las aplicaciones conocidas.
 4. Establecer las condiciones y las acciones que se realizarán cuando se repitan las actuales condiciones.
- c. El programa aplica la regla y la almacena para ocasiones sucesivas, clasificando la aplicación como permitida, bloqueada o con reglas.

En función de lo que hagamos en los pasos anteriores las aplicaciones quedarán clasificadas en:

- **Bloqueadas:** Todas las conexiones a Internet de este grupo se encuentran bloqueadas. Es recomendable incluir en este grupo las aplicaciones que no necesitan conexión a Internet, como editores de texto, calculadoras, etc. pero no olvides que si lo haces así y encuentras un documento de texto que incluye un enlace a una dirección en Internet no podrás acceder directamente a la misma desde el propio procesador de texto.
- **Aplicaciones con Reglas:** Todas las conexiones a Internet de este grupo se encuentran restringidas según la regla creada para cada aplicación y sólo serán permitidas las conexiones específicamente admitidas.
- **Aplicaciones permitidas:** Todas las conexiones a Internet de este grupo se encuentran permitidas.

Ante las alertas de seguridad de tu firewall, si no tienes muy claro qué hacer lo mejor es optar por decisiones que no sean definitivas y que te permitan ir observando lo que ocurre hasta que llegues a una conclusión sobre si la regla que debes adoptar es en la línea de permitir o denegar la conexión. Dentro de esta política de aprendizaje, siempre que te lo permita el cortafuegos que estés utilizando, podrías optar por Permitir una vez o Bloquear una vez. Parece lógico que si pretendes mantener tu seguridad mientras te dedicas a observar, lo más prudente es que optes por la opción de Bloquear el acceso en esta ocasión: si ves que el bloqueo no produce ningún efecto negativo ya tienes un elemento que te aproxima hacia uno de los criterios, mientras que si ves lo contrario y el programa vuelve a solicitarte permiso tal vez se deba a que la opción adecuada es conceder ese permiso.

Mientras no tengas claro si debes conceder permiso a una aplicación es preferible que sigas haciendo pruebas bloqueando el acceso cada vez que se produzca una petición. Ten en cuenta que, una vez establecida una regla se aplicará automáticamente sin volver a consultarte.

Uno de los problemas más frecuentes cuando se utiliza un programa cortafuegos es que indiquemos erróneamente el bloqueo permanente de una aplicación y si ésta es nuestro navegador... No te preocupes, lo que tendrás que hacer es ir a las opciones de programa y desbloquear y dar permisos de accesos a dicho programa.

Vamos a describir en primer lugar el firewall de Windows 7 que al estar incorporado en el propio sistema operativo de Microsoft ofrece una perfecta integración y gestión de los recursos del propio sistema.



Atención

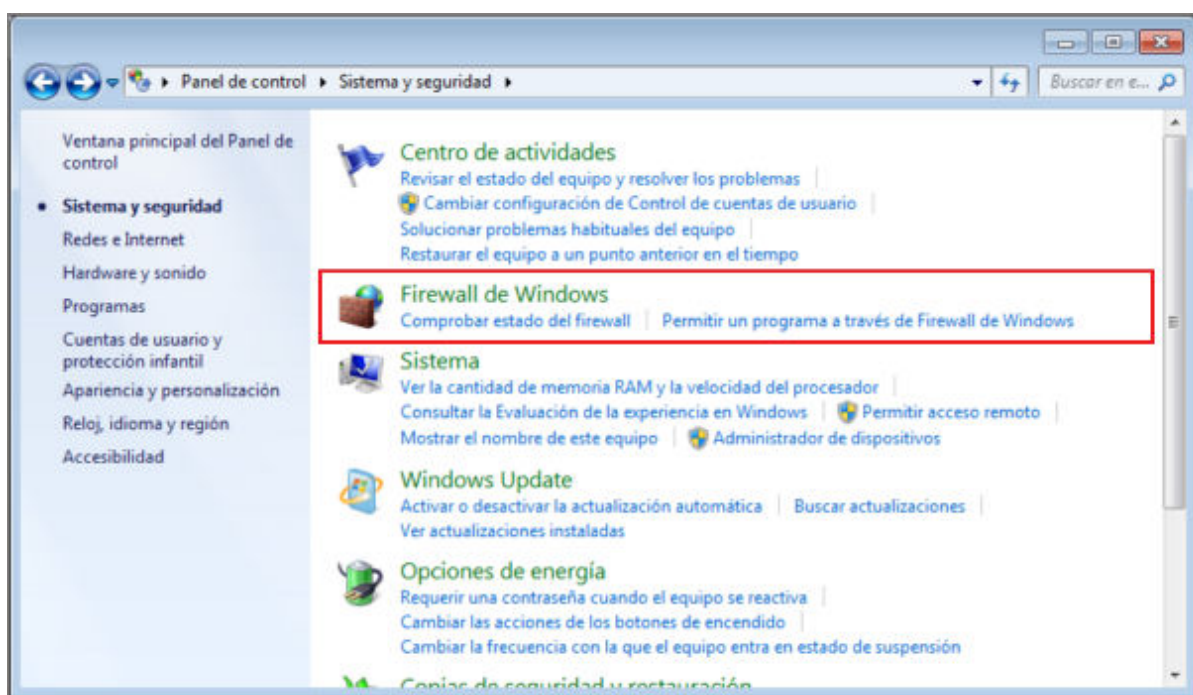
No es conveniente tener más de un cortafuegos ejecutándose al mismo tiempo en un mismo sistema operativo, así que si tienes uno instalado, y no te gusta, lo recomendable es desactivar uno antes de instalar otro.

Firewall de Windows 7

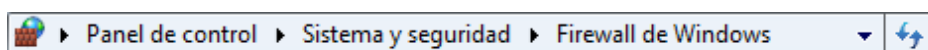
Posiblemente el hecho de que Microsoft incorpore en tu sistema operativo Windows un cortafuegos (firewall) sea motivo de confianza para no tener que desactivarlo y utilizar otro, así que vamos a describirlo en su versión de Windows 7.

El Firewall de Windows 7 al estar incorporado en el propio sistema operativo de Microsoft ofrece como ventaja principal una perfecta integración y gestión de los recursos del propio sistema.

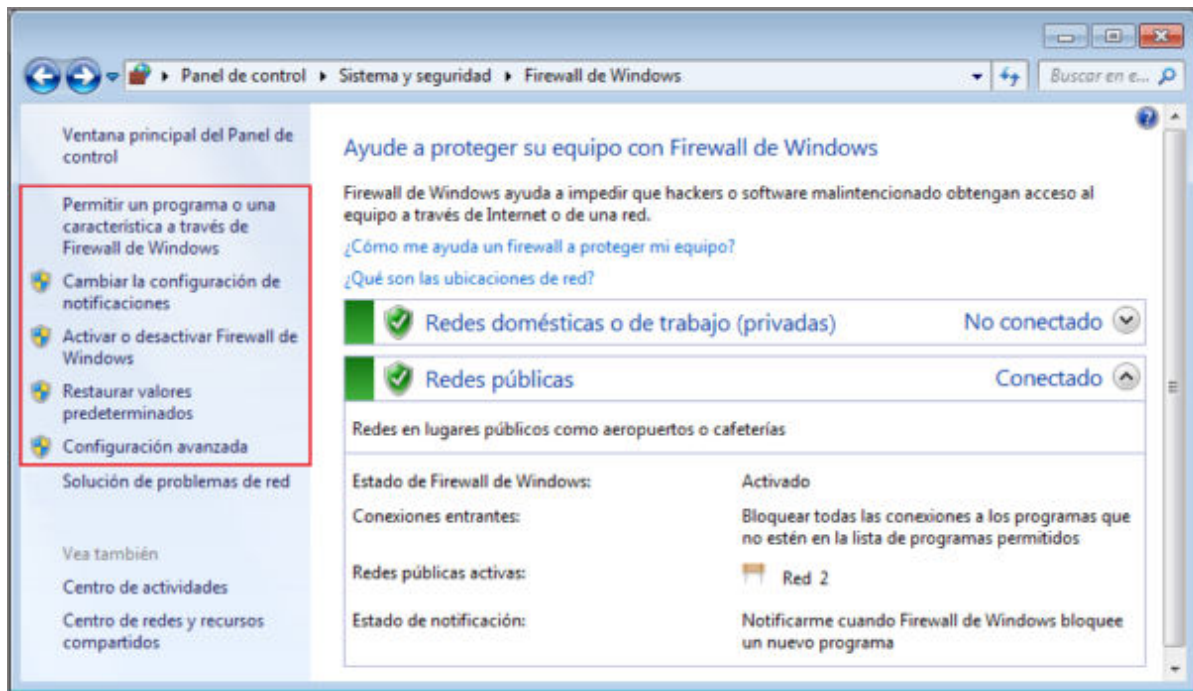
Para la localización del Firewall de Windows 7 sólo tendrás que seguir los siguientes pasos: **Inicio ➔ Panel de Control ➔ Sistema y seguridad** y se te mostrará la siguiente pantalla donde podrás acceder a las funcionalidades del Firewall de Windows.



En la barra de dirección encontrarás la "miga de pan", es decir el camino, recorrido hasta localizar esta aplicación de Windows:

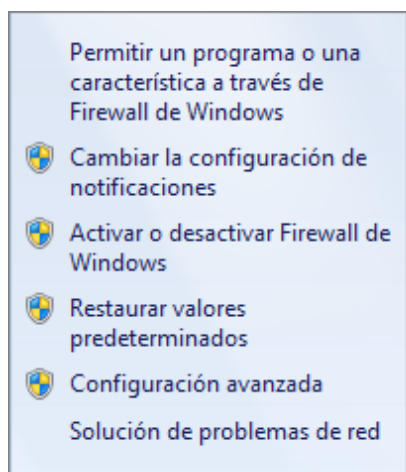


El manejo es bastante sencillo e intuitivo, y simplemente pulsando sobre el enunciado **Firewall de Windows** podrás acceder a su menú de opciones y visualización de la configuración.

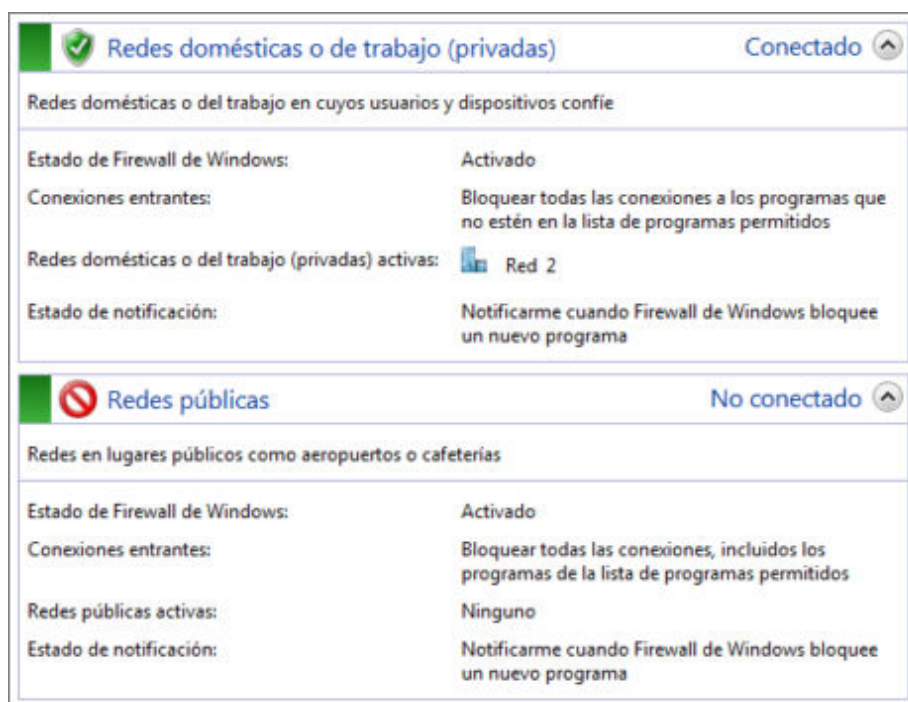


La ventana de Firewall te mostrará:

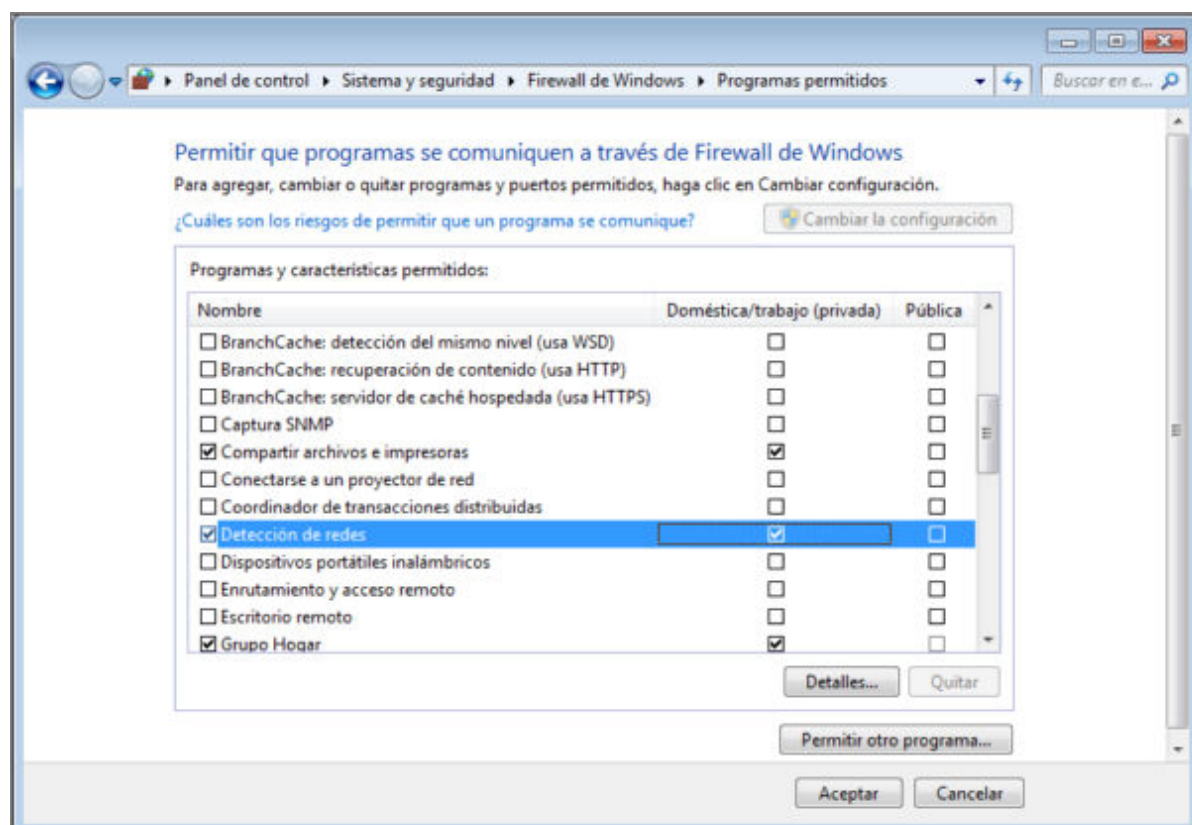
- **El menú de opciones**, situado en el marco izquierdo de la ventana, desde el que podremos seleccionar todas las funcionalidades del Firewall:




- El **estado de nuestro Firewall**, en la zona principal de la pantalla, nos dará la información de la configuración establecida respecto a las redes privadas y públicas sobre:
 - Si está conectado o no.
 - Si tenemos activo o no el Firewall.
 - Si bloqueamos o no todas las conexiones entrantes, incluidas las permitidas.
 - Si queremos que se nos notifique o no cuando se bloquee un nuevo programa.

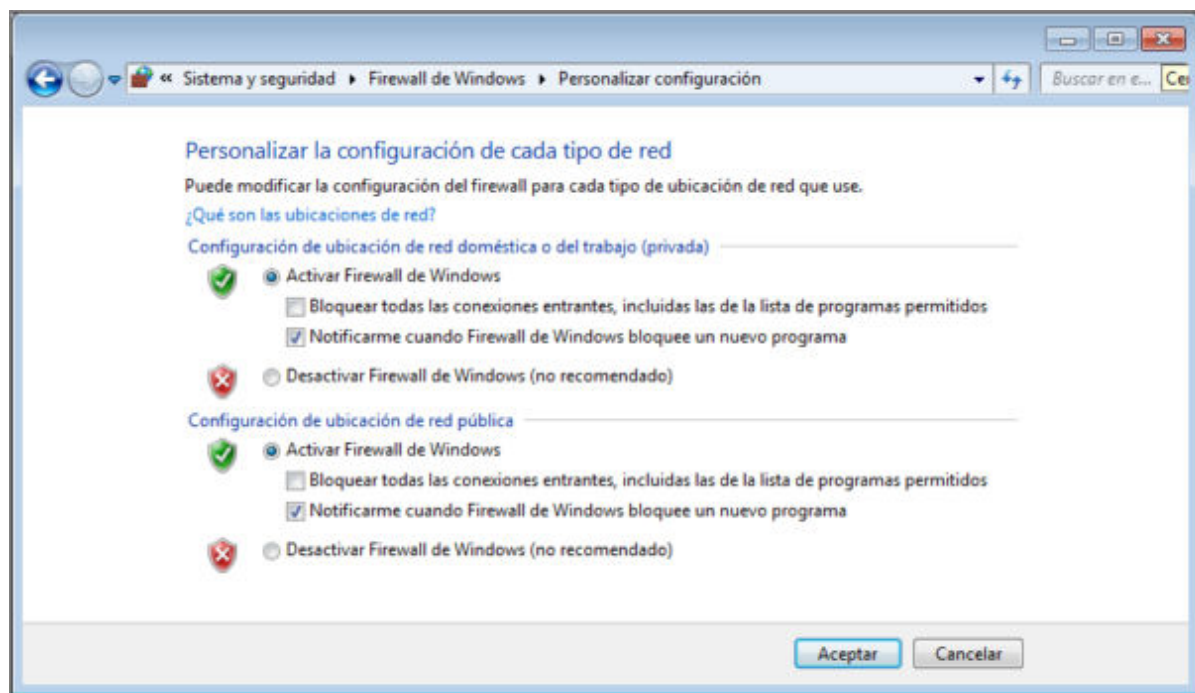


La primera opción es la configuración de los **permisos de programas a través de Firewall de Windows**, pudiendo ver los detalles de cada uno de ellos, activar el cambio de configuración o realizar nuevos permisos de otros programas que queramos añadir.



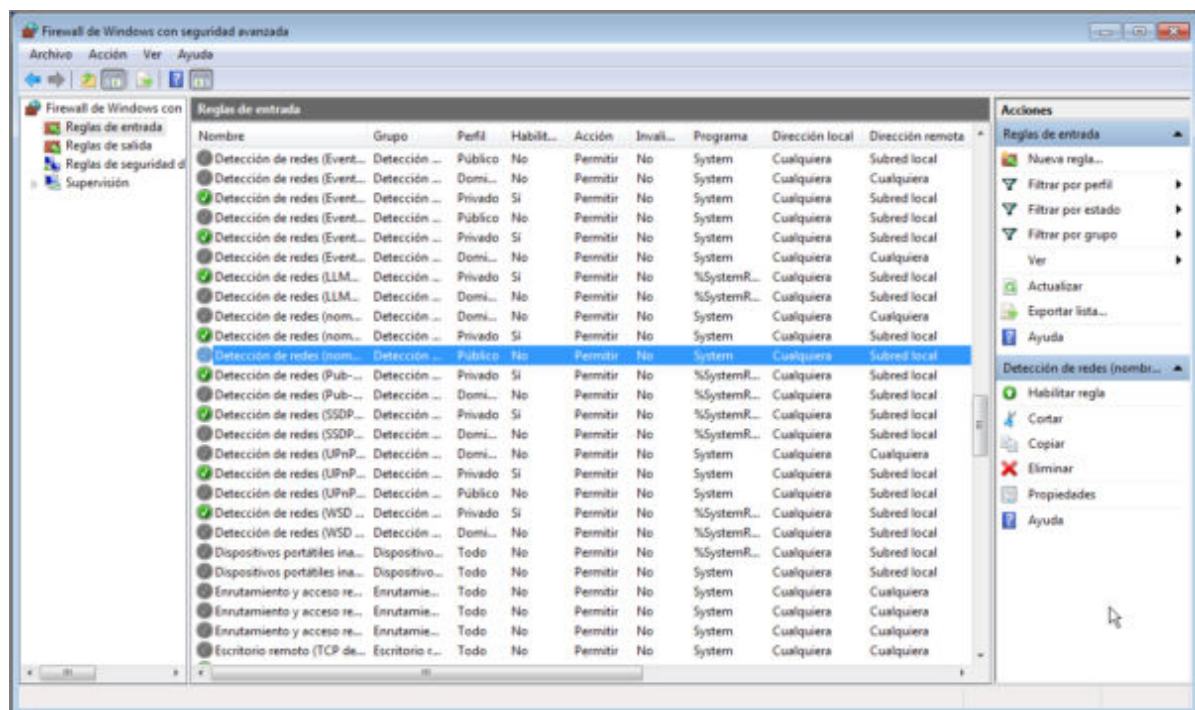
Con la segunda y tercera opción podremos optar por **Cambiar la configuración de notificaciones** o **Activar o desactivar Firewall de Windows**. Ambas opciones del menú nos llevan a la personalización de la configuración para elegir, activando o desactivando sus opciones, cualquiera de las posibilidades comentadas anteriormente. La configuración establecida se nos representará gráficamente como **Firewall activado** , **Firewall**

desactivado  o Bloqueo de todas las conexiones entrantes .



También podremos activar siempre que queramos la opción **Restaurar valores predeterminados**, lo que nos devolverá a la configuración de origen del sistema.

La siguiente opción del menú de Firewall de Windows es el acceso a la **Configuración avanzada** que nos posibilitará una gestión más personalizada de cada una de las reglas establecidas pudiendo, además de tener una visión más pormenorizada de cada una de ellas, habilitarlas o deshabilitarlas, cortarlas, eliminarlas,....



Cada vez que Windows intercepte una conexión o programa que no tenga contemplado en sus permisos nos lo comunicará si así se lo hemos establecido.



La última opción del menú de opciones, aunque no forma parte de las opciones de Firewall de Windows, permite ayudar a solucionar problemas de red para que las conexiones funcionen correctamente y el Firewall pueda ser efectivo.


ZoneAlarm

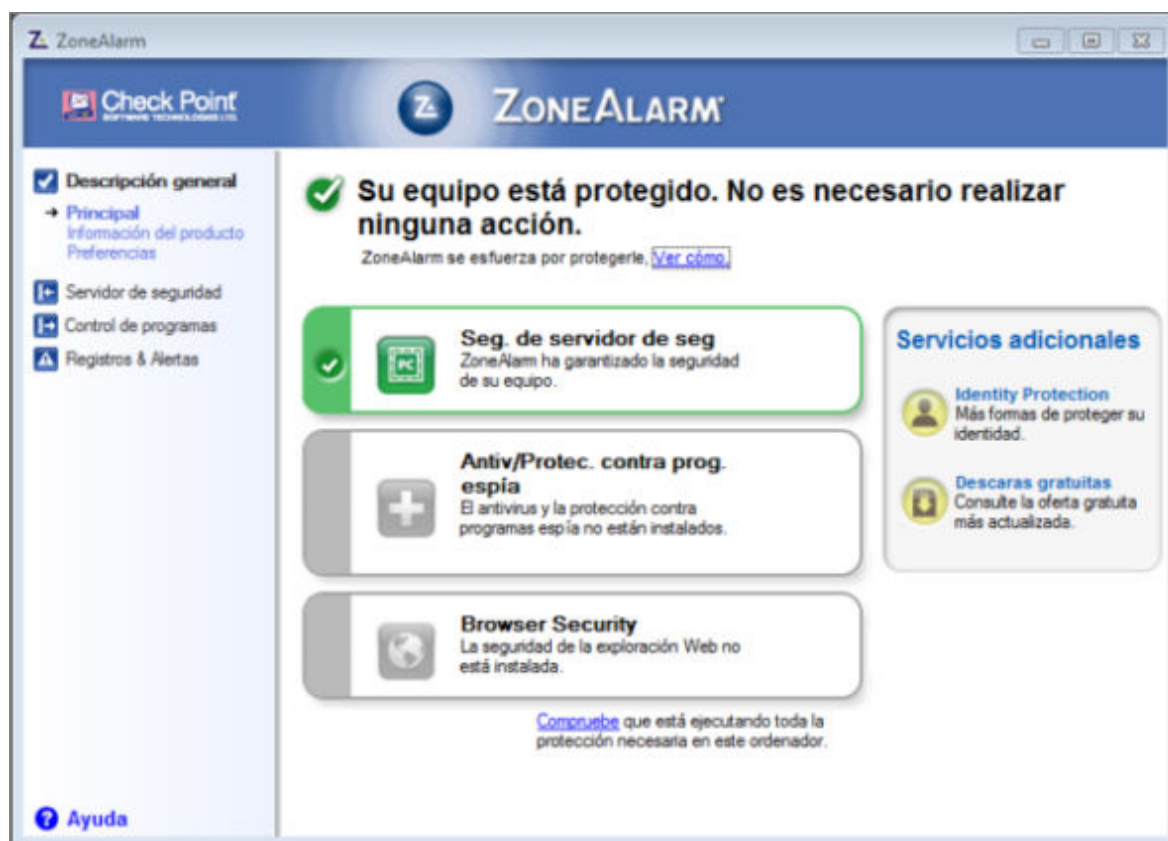
Dentro de la diversidad de programas cortafuegos, existen muchos programas comerciales que ofrecen multitud de prestaciones, pero también existen versiones freeware que aportan una funcionalidad bastante completa. Seguidamente describiremos la utilización del firewall de **ZoneAlarm** para entorno Windows que dispone de una versión totalmente gratuita. Si quieres buscar y probar algún software diferente puedes buscar en Softonic la sección dedicada a cortafuegos para Windows o Linux.

ZoneAlarm es una versión gratuita de firewall, compatible para el sistema operativo Windows 7, cuyo funcionamiento no es muy diferente al firewall del propio sistema operativo comentado anteriormente.

Como la versión con la que trabajamos es la que se distribuye gratuitamente, encontrarás diversas opciones desactivadas y enlaces que te referenciarán a otras versiones de pago del propio programa. Puedes descargar el programa desde [softonic](#) en la sección de cortafuegos, gratis y en español, o desde la propia página web de [Zone Alarm: Descargue ZoneAlarm Gratuito](#).



Para la instalación sólo tendrás que elegir entre la modalidad rápida (realizada por el propio programa) o personalizada, aceptar el contrato de licencia de uso y tras la instalación de los ficheros te pedirá reiniciar el sistema para concluir el proceso. Después de reiniciado el sistema se activará **ZoneAlarm** y encontrarás el icono del programa  en la barra de tareas.



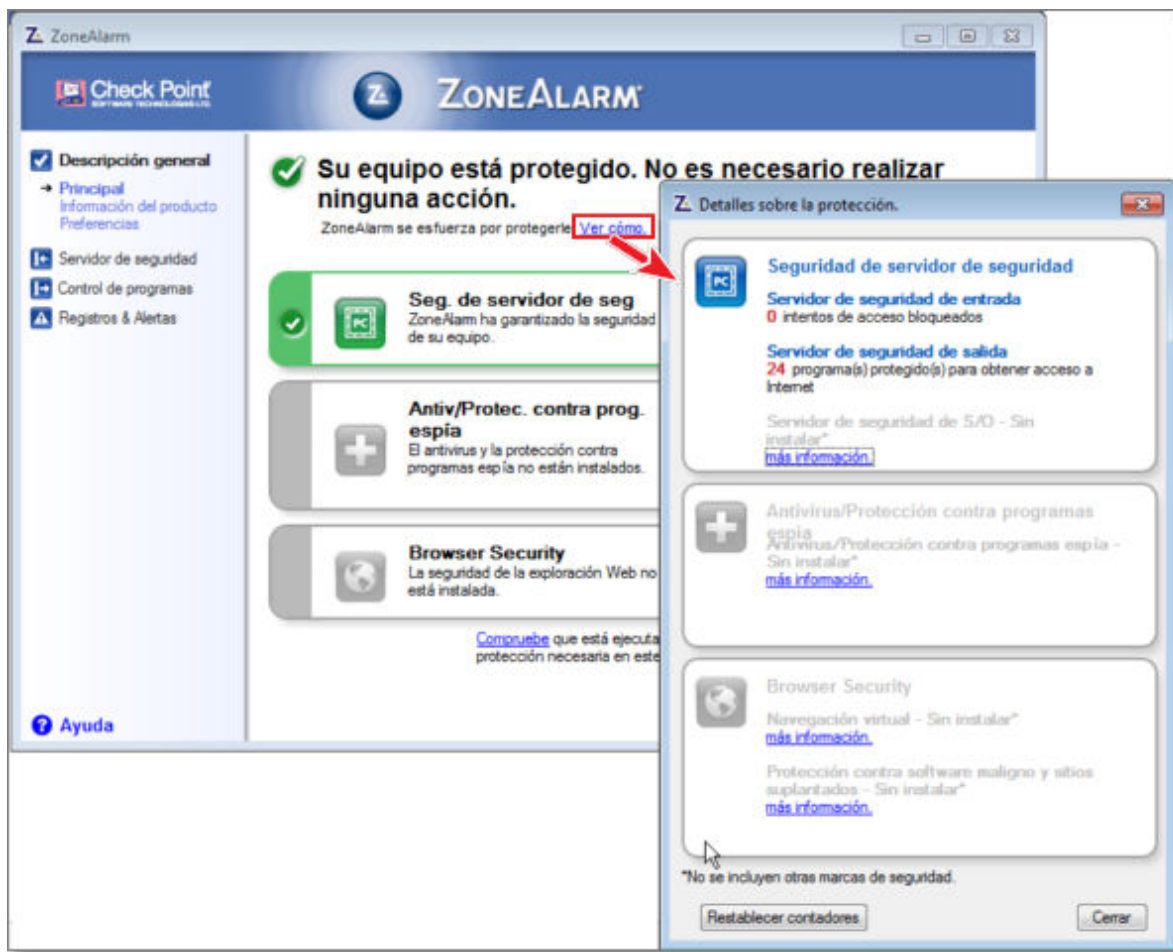
En el momento que cualquier programa quiera acceder a la red aparecerá una alerta de seguridad del programa para que determines su permiso o denegación.



En la alerta puedes permitir o denegar el acceso recordar e igualmente Recordar la configuración para que quede guardada y ya no nos vuelva a preguntar. De esta forma irás enseñando al ZoneAlarm los permisos sobre cada uno de los programas que intenten acceder, de forma que al principio te preguntará por todos pero poco a poco se irá limitando a

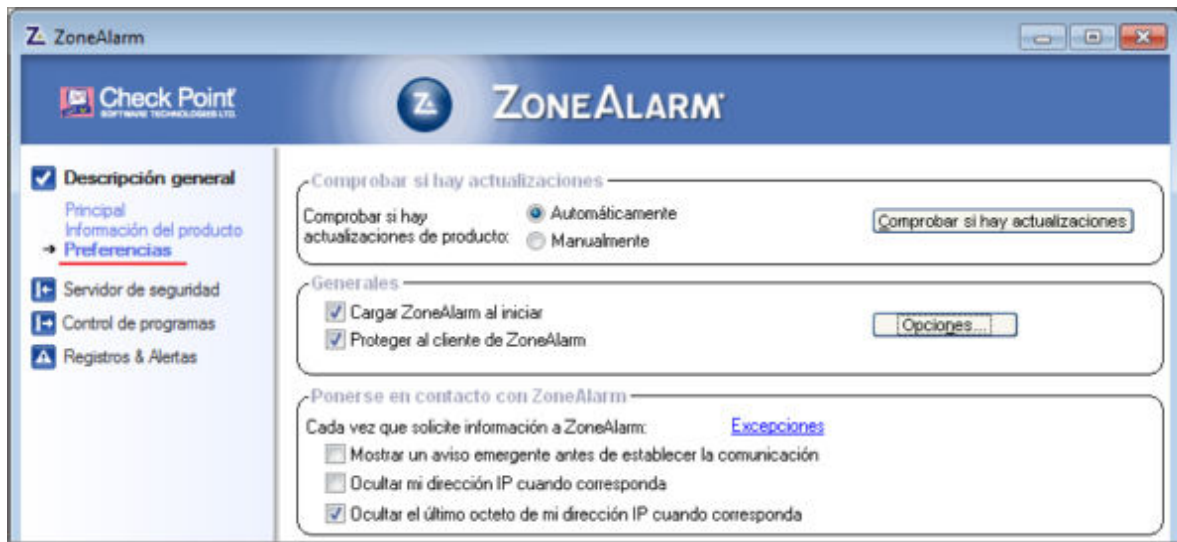
aquellos que no tiene contemplados.

Desde la pantalla principal del Centro de control de ZoneAlarm podemos tener un resumen de la protección realizada.



También desde esta pantalla principal nos informa que sólo tenemos instalada la parte del programa de **Seguridad de servidor de seguridad** que es la que está disponible en esta versión gratuita. Desde **Seguridad de servidor de seguridad** también podemos acceder a un resumen y a los enlaces al control sobre zonas y programas.

En la siguiente opción de **Descripción general ➔ Preferencias** podrás configurar el modo de actualización y de activación de ZoneAlarm. En condiciones generales interesa tener una actualización automática del programa y una protección desde el iniciar de ejecución del sistema operativo.



En el apartado de **Servidor de seguridad** podrás seleccionar 3 niveles de seguridad (Alto, Medio y Desactivado) para cada una de las zonas:

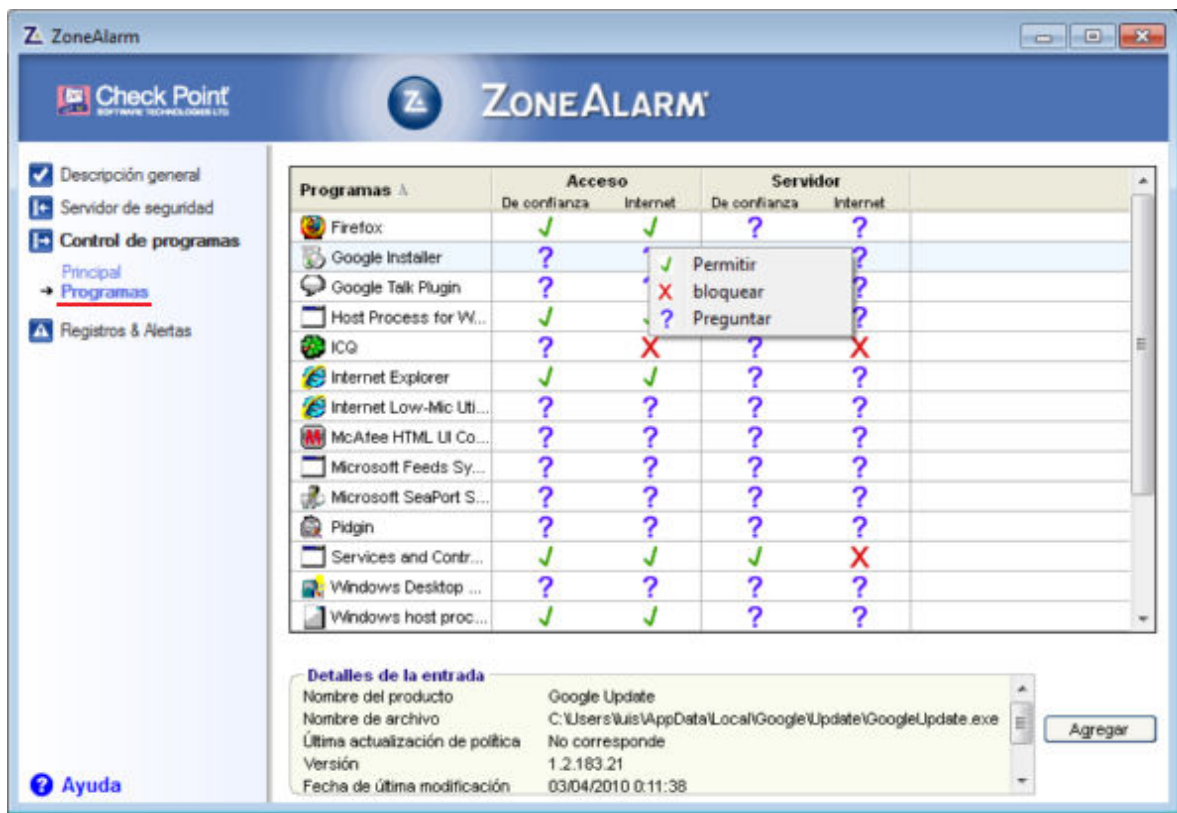
- Zona de Internet: para redes públicas que no sean de confianza.
- Zona de confianza: para redes privadas de trabajo o casa que se entiende que son de mayor confianza y seguridad.



En la siguiente opción del menú lateral podrás gestionar el **control de los programas** mediante un menú principal que permite la configuración de cuatro niveles (Alto, Medio, Bajo y Desactivado) de acceso a Internet y derechos de servidor, para programas que además de enviar datos también los reciben (actúan como servidor).



Pulsando con el botón izquierdo del ratón puedes controlar **cada uno de los programas** configurando de forma particular el permiso, bloqueo o que te pregunte qué hacer cuando realice el acceso. Igualmente pulsando con el botón derecho podrás agregar o borrar programas del listado.



La última opción de **Registros y Alertas** te permitirá tener una información completa de las tareas realizadas. En **Principal** podrás configurar la posibilidad de guardar el registro del programa e indicar dónde y cómo guardarlo; mientras que la opción **Visor de registros** te mostrará un informe detallado de cada uno de los accesos y medidas adoptadas por el programa.

Check Point
SOFTWARE TECHNOLOGIES LTD.

ZONEALARM

☒ Descripción general
 ☐ Servidor de seguridad
 ☐ Control de programas
 ☒ **Registros & Alertas**

Principal
 → [Visor de registros](#)

Ayuda

Mostrar último: 50

Tipo de alerta: Programa

Clasificación	Fecha / Hora	Tipo	Programa	IP de origen	IP de destino
Alto	2010-05-03 18:54:04+...	Programa repetido	C:\Program File...		80.58.61.250.5
Medio	2010-05-03 18:53:58+...	Acceso de progra...	GoogleUpdate....		209.85.227.13
Alto	2010-05-03 18:53:58+...	Programa repetido	C:\Users\uis\A...		209.85.227.13
Medio	2010-05-03 18:53:58+...	Acceso de progra...	GoogleUpdate....		209.85.227.11
Alto	2010-05-03 18:53:58+...	Programa repetido	C:\Users\uis\A...		209.85.227.11
Medio	2010-05-03 18:53:58+...	Acceso de progra...	GoogleUpdate....		209.85.227.10
Alto	2010-05-03 18:53:58+...	Programa repetido	C:\Users\uis\A...		209.85.227.10
Medio	2010-05-03 18:53:58+...	Acceso de progra...	GoogleUpdate....		209.85.227.13
Alto	2010-05-03 18:53:58+...	Programa repetido	C:\Users\uis\A...		209.85.227.13
Medio	2010-05-03 18:53:58+...	Acceso de progra...	GoogleUpdate....		209.85.227.10
Alto	2010-05-03 18:53:58+...	Programa repetido	C:\Users\uis\A...		209.85.227.10
Medio	2010-05-03 18:53:58+...	Acceso de progra...	GoogleUpdate....		209.85.227.10
Alto	2010-05-03 18:53:58+...	Programa repetido	C:\Users\uis\A...		209.85.227.10

Detalles de la entrada

Descripción
 Google Installer was unable to obtain permission for connecting...

Clasificación
 Medio

Fecha / Hora
 2010-05-03 18:53:58+2:00

Tipo
 Acceso de programas

Agregar a zona>>

Más información

Borrar lista

Spyware o programas espías

Otro problema de seguridad con el que nos podemos encontrar son los **programas espías** (en inglés **spyware**). Básicamente son programas que se instalan en nuestro ordenador sin nuestro consentimiento y nos roba información sin que nos demos cuenta.

Te mostramos en este bloque qué son y cómo puedes defenderte.



¿Qué es?

Quizás ya sepas que hay posibilidad de descargar una buena cantidad de programas de forma gratuita de Internet, y que algunos de ellos, los que se denominada adware, ofrecen las prestaciones de las versiones comerciales a base de reservar una parte de la pantalla para la presentación de anuncios publicitarios.

Aparentemente, el único compromiso que adquiere el usuario de uno de estos programas es permitir la aparición en su pantalla de publicidad cuya visita no es obligatoria. Pero, en muchos casos la realidad no es tan inocente como aparenta y, además de ese pequeño banner publicitario, se instala en el ordenador un programa que se encarga de monitorizar las páginas de Internet que se visitan y enviar esa información a empresas especializadas en el análisis de datos, siempre sin conocimiento por parte del usuario de que este hecho se está produciendo. Dichas empresas se encargan de ir afinando los perfiles de cada usuario para vender esos datos a las grandes corporaciones publicitarias y posibilitar la segmentación de la publicidad, de forma que los mensajes que nos vayan llegando se adecuen cada vez más al perfil que traslucimos a través de la navegación por la red.

Este tipo de programas espía se denominan en terminología anglosajona spyware y su introducción por esta vía es muy poco frecuente entre los programas de software libre, ya que al ser obligatoria la distribución junto con el código del programa cualquier programador podría descubrirlos y modificarlos.

Otra forma de que se introduzcan espías en nuestro navegador es a través de la visita a páginas que incluyen en su código las instrucciones para almacenar en nuestro ordenador una "cookie". Estas "galletitas" son pequeños fragmentos de código entre cuyas funciones puede estar la de determinar los intervalos entre una y otra visita, el número de veces que se visita la página, etc.

Les hay que tiene propósitos más perversos como la localización en nuestro ordenador de datos de conexión, teléfono, claves y contraseñas de accesos a correos y sitios privados, nuestro software, nuestros contactos, etc. Por todo ello es bueno tomar las medidas, ya comentadas en esta documentación, de seguridad en nuestra navegación por Internet: no abrir mensajes desconocidos o sus ficheros adjuntos, no acceder a direcciones de pantallas de popups no elegidas, no instalar programas no sean legales o de sitios de confianza, etc.

Vamos a comentarte cómo defenderse ante este tipo de intromisión de nuestra privacidad sin nuestro consentimiento.

¿Como defenderse?

Si quieres defenderte de estos espías puedes utilizar algunos programas antivirus que incorporan también esta protección de spyware o programas específicos que puedes descargar gratuitamente desde la red.

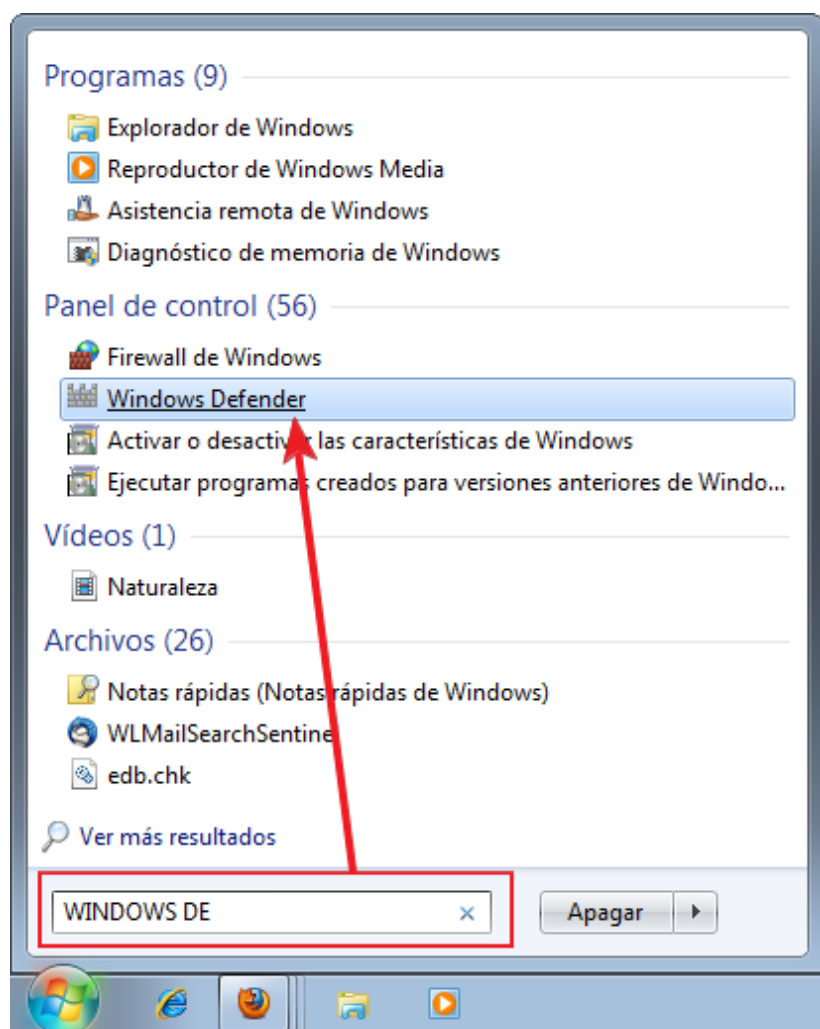
Veremos seguidamente un programa integrado y distribuido por el propio Windows (Windows Defender) y otro programa independiente que posee una versión gratuita (Ad-Aware).

Windows Defender en Windows 7

Al igual que hemos comentado en el apartado de cortafuegos, Microsoft ha incorporado y activado por defecto en los sistemas operativos Windows Vista y 7 su propio sistema de protección de spyware llamado Windows Defender. Para Windows XP también existe versión y tienes la posibilidad de descargar Windows Defender desde la propia página oficial de Microsoft.

Las posibilidades que ofrece Windows Defender no difieren de las que podrás encontrar en cualquier otro programa antispyware, (análisis de antispyware, avisos, eliminación, cuarentena,...), aunque en este caso posee una integración plena con Internet Explorer.

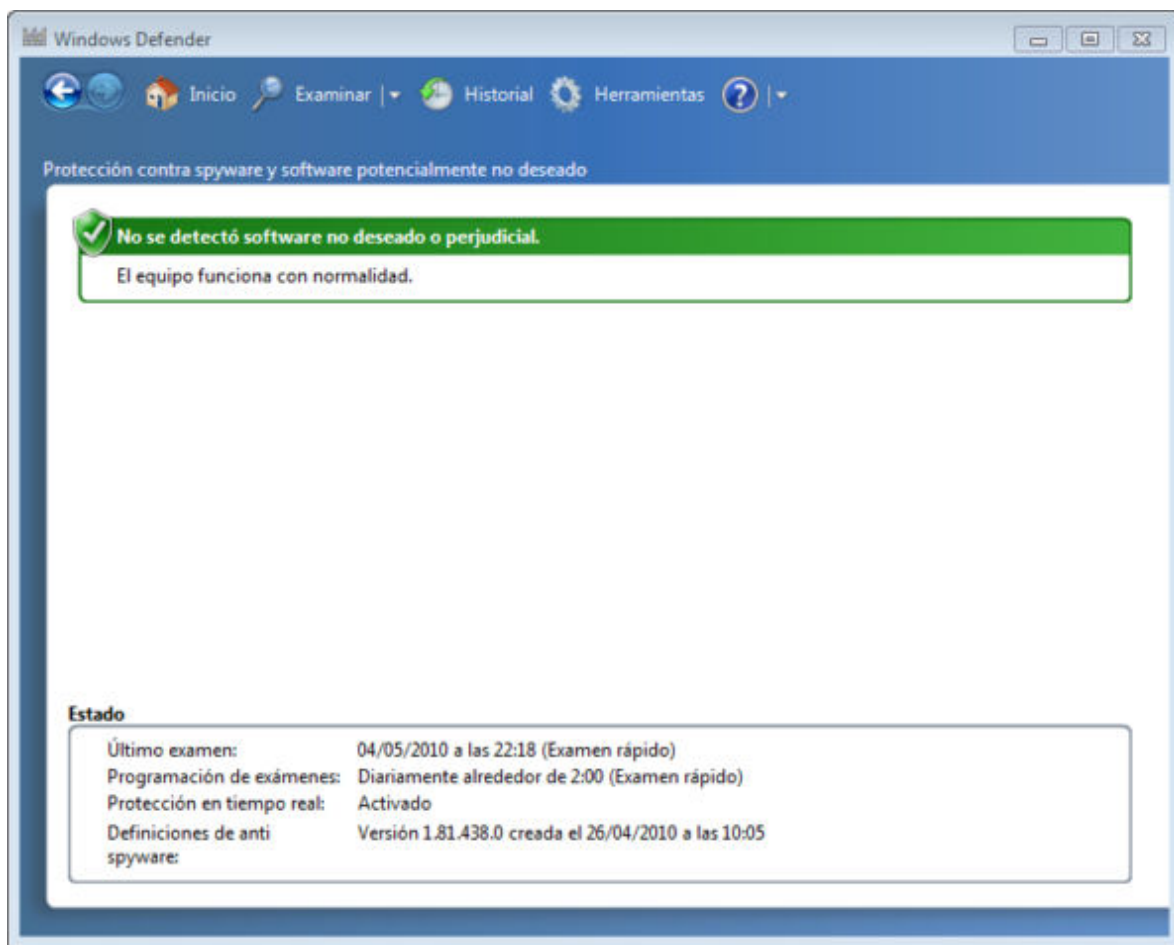
El modo más sencillo de localizar Windows Defender es desde **Inicio**  ➡ **Buscar programas y archivos**  escribiendo el nombre del programa.



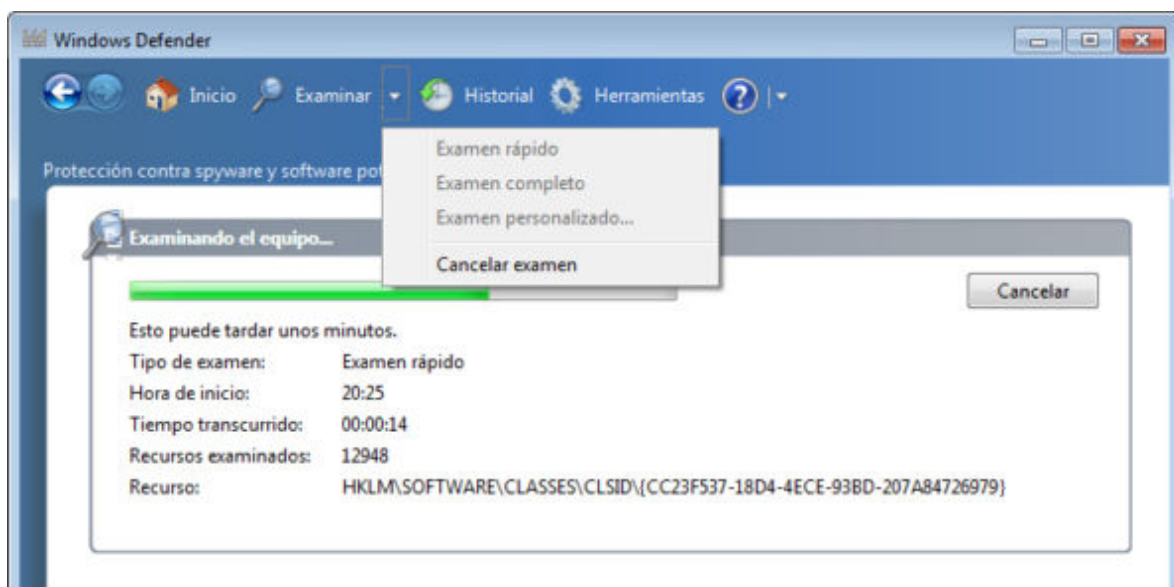
Tras seleccionar el programa se abrirá la ventana de **Inicio**. En la parte superior se encuentran todas las opciones principales: Inicio, Examinar, Historial, Herramientas y Ayuda. En la zona central nos informa del funcionamiento del programa y de su estado:

- **Ultimo examen realizado,**
- **Programación establecida para la realización de exámenes,**

- Estado de protección en tiempo real,
- Versión de la definición de anti spyware.



Con la opción **Examinar** podrás seleccionar si deseas que ésta se realice de forma rápida, completa o personalizada (seleccionando las unidades a examinar) para detectar los posibles archivos spyware que podamos tener en nuestro ordenador. Al final del examen te presentará un resumen de las estadísticas del trabajo realizado.



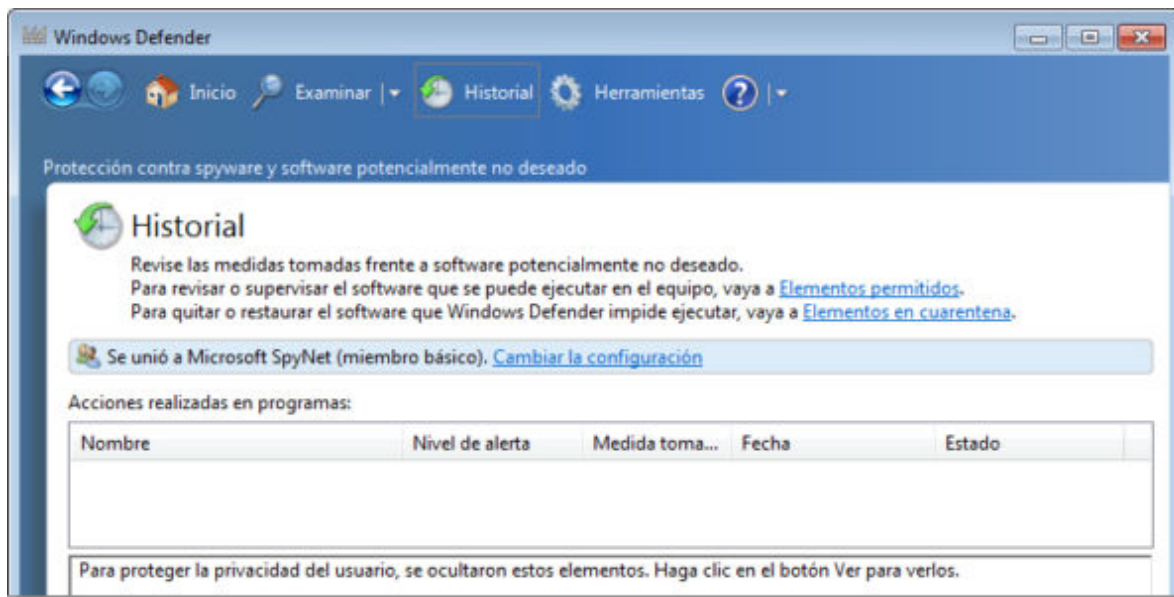
Mediante el **Historial** podrás visualizar los archivos localizados y las acciones o medidas tomadas. Podrás visualizar el Historial de los elementos permitidos y los que están en

cuarentena.

Los archivos permitidos son aquellos que, aunque el programa a considerado que pueden ser perjudiciales, has decidido permitir su ejecución siempre, no volviendo el programa a preguntar por ellos mientras se encuentren en esta lista de permitidos.

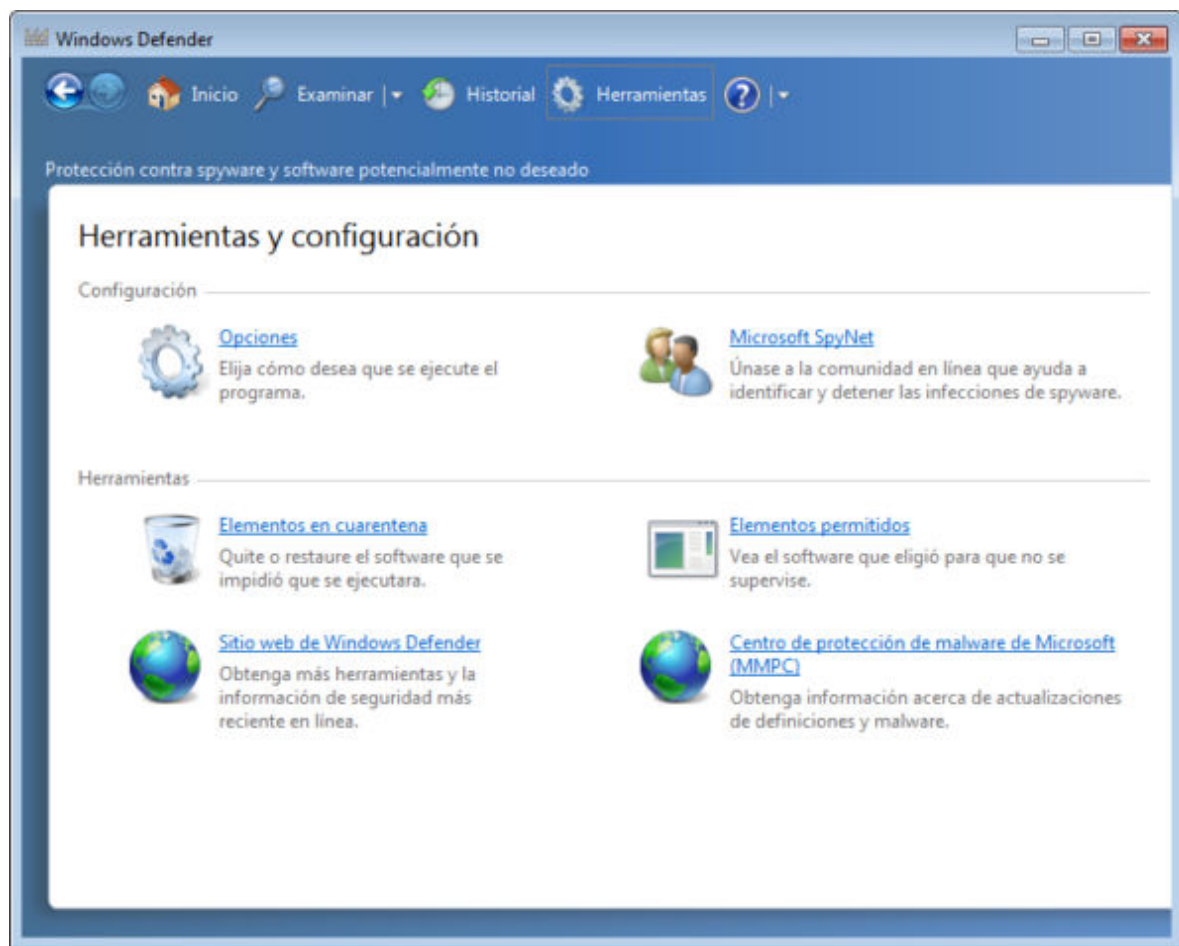
Los archivos situados en cuarentena son aquellos sobre los que tienes dudas y estarán en esa lista hasta que decidas restaurarlos o eliminarlos.

En esa misma pantalla del Historial, tras seleccionar un archivo, podrás visualizar una descripción de cada uno de los ficheros localizados lo que te permitirá tener más información para tomar tu decisión de la acción a realizar sobre él.

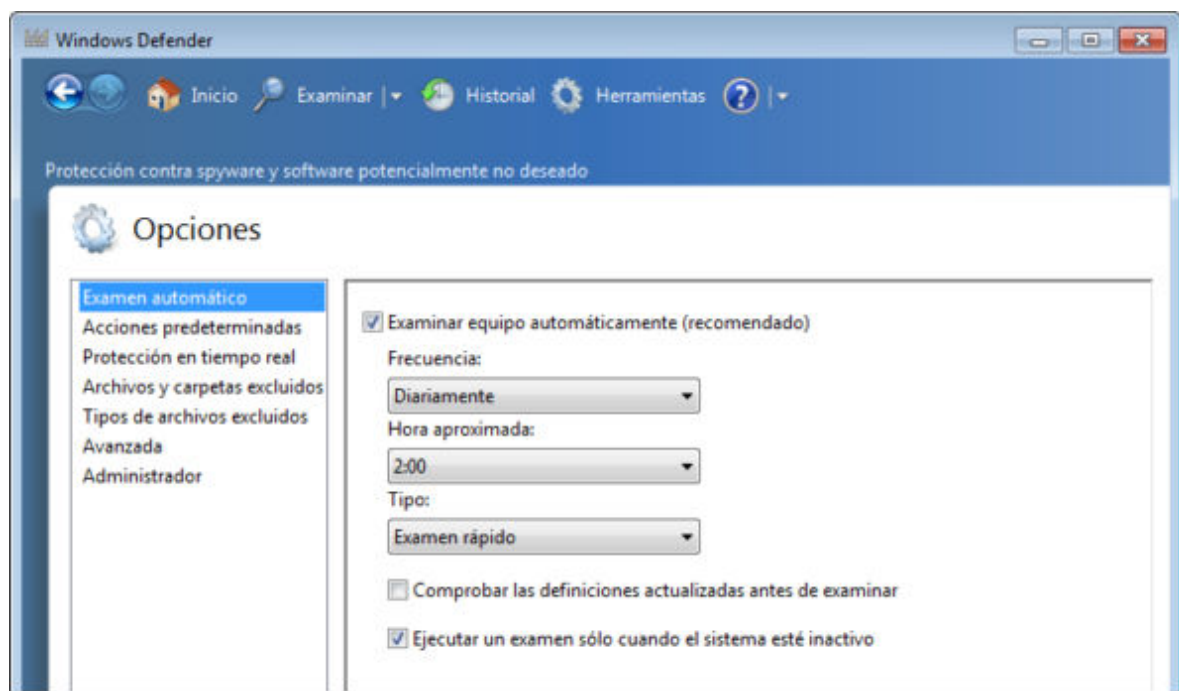


Con la opción **Herramientas** podrás en configurar y acceder a herramientas del programa.

En **Herramientas** puedes visualizar de nuevo el listado de elementos en cuarentena y permitidos y conectarte directamente a la web de Windows Defender y de malware de Microsoft para estar informado de las últimas noticias que sobre temas de seguridad ofrece Microsoft.

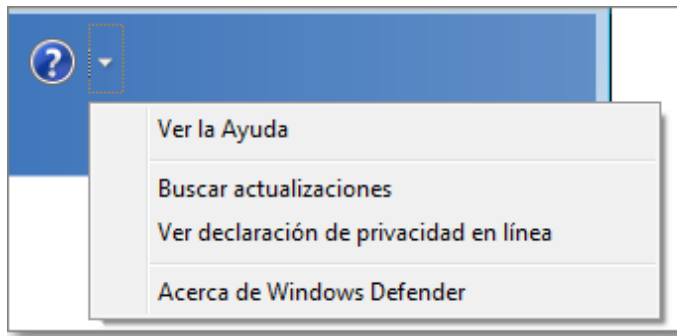


Desde **Opciones** es verdaderamente donde podrás configurar el modo de funcionamiento del programa (programar el examen automático, acciones determinadas, la protección en tiempo real, archivos, exclusiones,...) y, si lo deseas, unirse a la comunidad online de Microsoft SpyNet para colaborar en la identificación y detección de malware.



Con la última opción de **Ayuda** podrás acceder a la Ayuda y soporte técnico pulsando en la interrogación o seleccionar otras posibilidades desplegando el menú de la flecha adjunta:

ayuda, actualizaciones, declaración de privacidad o versión de Windows Defender.



Para aquellos usuarios de Windows, Microsoft también ofrece de forma gratuita un antivirus llamado [Microsoft Security Essentials](#) (MSE). Como antivirus es menos efectivo que otros programas especializados que hemos comentado en el apartado de antivirus, pero entre sus posibilidades está la eliminación también de spyware. En su instalación reemplaza a Windows Defender por estar incorporada también en el propio programa de MSE la detección de spyware.



Práctica


Si estás usando el sistema operativo Windows, activa Windows Defender para realizar un examen rápido contra spyware.

Ad-Aware


Si piensas que es mejor contar con un programa distinto al del propio Windows, puedes buscar y descargar de Internet otras opciones, algunas gratuitas y en castellano.

Te presentamos seguidamente una de ellas: **Ad-Aware** en su versión gratuita.

Para descargarte el programa, puedes conectarte a www.adaware.es, y pulsar sobre el icono

de **Ad-Aware FREE** . El siguiente paso es que te pedirá rellenar el cuestionario que te presentan y ya podrás descargar el programa.

La instalación es muy sencilla, al ejecutar el programa de instalación tendrás que seleccionar el idioma deseado y, tras la aceptación de los términos del contrato de licencia, continuar los pasos que te indica el asistente de instalación. Al finalizar la instalación, se te pedirá reiniciar el sistema para completar la instalación.

Al reiniciarse el sistema, Ad-aware primero se actualizará y después se ejecutará y quedará indicado en la barra de sistema  16:29.




La primera pantalla que nos muestra el programa es la de registro, pero dado que nuestra versión es la gratuita (para uso particular) no nos registramos.

La ejecución del programa es muy intuitiva. Como muy bien te informa en su pantalla de bienvenida, lo primero que deberás hacer es elegir el modo de utilización de Ad-aware:



- En el **modo simple**: el programa gestiona automáticamente la detección y eliminación de las amenazas detectadas.
- En el **modo avanzado**: podrás decidir la configuración, detección y eliminación de las amenazas.



Es muy importante que tengas al día tu programa de Ad-aware con la opción **Actualización web**  pues de ello dependerá la eficacia de dicho programa.



Si queremos ejecutar el programa la opción es **Analizar** y podremos optar por una análisis inteligente (comprobación rápida del sistema y de las secciones más críticas) o un análisis completo (en profundidad de todo el sistema y de todas sus unidades locales).

Si estás en el modo avanzado, puedes utilizar el botón  **Configurar.** para modificar las preferencias, aunque encontrarás que algunas opciones están marcadas en gris puesto que sólo es posible habilitarlas cuando se utiliza alguna de las versiones comerciales. Una vez que hayas establecido los discos que quieres revisar y cualquier otro tipo de preferencia puedes iniciar la revisión pulsando 




Cuando se complete el proceso aparecerá una pantalla resumen en la que nos informa de los espías localizados y podremos optar por:

- **Realizar una acción global:** desplegando la flecha de Action de la barra de resultados podremos seleccionar **Personalizada** (cada uno puede tener una acción distinta), **Todo Cuarentena** (los mete en la carpeta cuarentena como precaución), **Quitar todo** (eliminar), **Reparar todo** (el programa intentará poner soluciones a las referencias encontradas), **Todo una vez** (los permite por esta vez) o **Añadir todo a ignorar** (los deja de reconocer como malware).



- **Realizar acciones individuales** con cada uno de ellos, seleccionando en cada uno la opción que queramos (**Quitar**, **Permitir una vez** o **Añadir a ignorar**).



Una vez que tengas seleccionada la acción global o marcadas las opciones individuales en cada uno de los objetos pulsa el botón **Realizar acciones**  y se ejecutarán las acciones.

Ten en cuenta que la acción por defecto del programa es la eliminación de los objetos encontrados y algunos programas pueden dejar de funcionar si se elimina el archivo espía que instalan. Por eso, si no tienes muy claro si te conviene eliminarlos o no puedes jugar con las otras opciones que te ofrece el programa. De todas maneras, habiendo muchos programas con licencia GNU/GPL o freeware que pueden hacer funciones similares, casi te recomendamos que busques otro programa que pueda realizar las mismas funciones y abandones el que instaló un espía.

El programa también cuenta con un módulo llamado Ad-Watch Live que permite la detección de spyware en tiempo real de forma que está siempre monitorizando los posibles intrusos.



Práctica

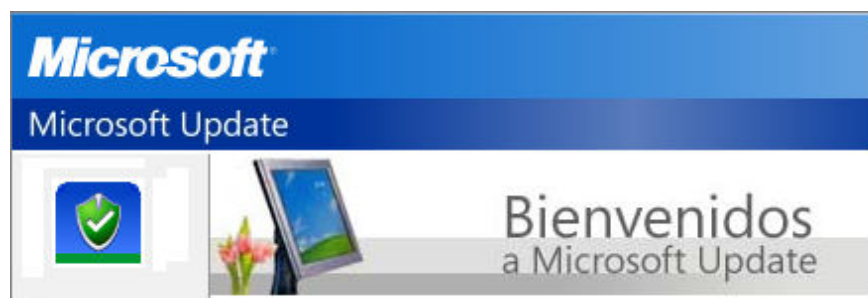
Ejecuta Ad-aware para limpiar tu sistema de indeseables espías.

Windows Update

Una de las cuestiones esenciales en cuanto a seguridad cuando trabajas con un sistema operativo Windows es la descarga e instalación de las actualizaciones.

Microsoft, al igual que la mayoría de los fabricantes y empresas de informática, utiliza Internet como medio de actualización y mejora de sus productos.


Si dispones de los sistemas operativos Windows XP, Windows Vista o Windows Vista 7 podrás utilizar el servicio de actualización automática para tener al día tu sistema.




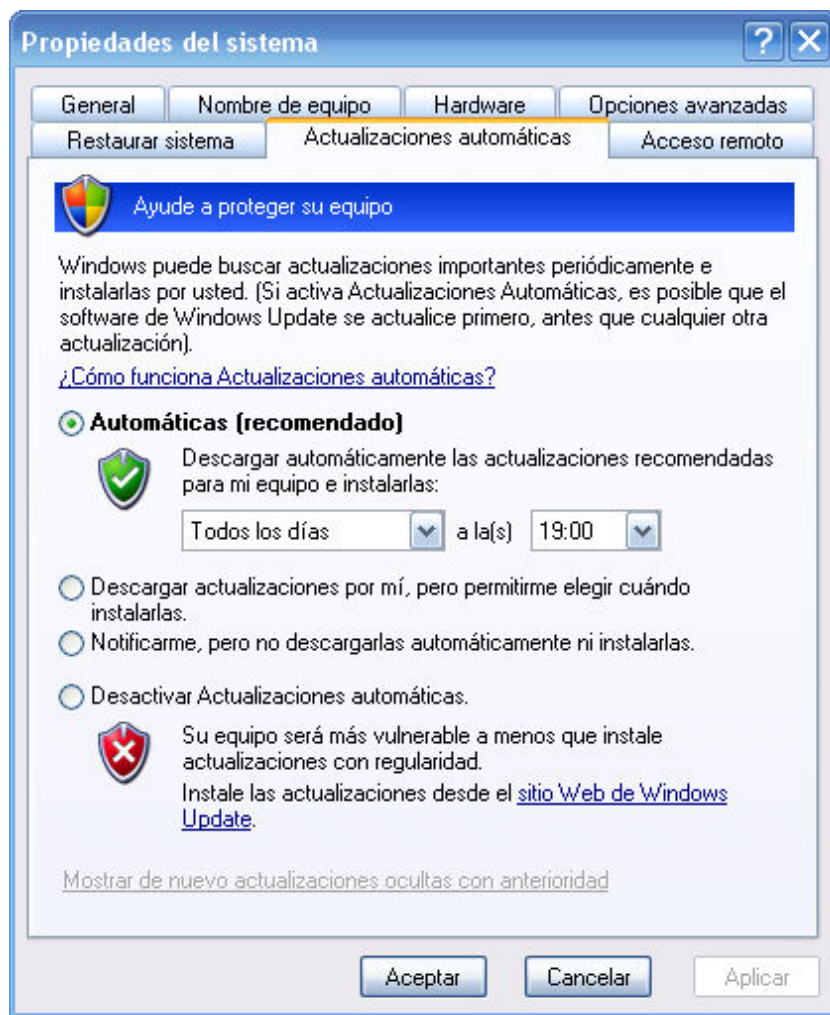
Atención

Para poder utilizar el servicio de actualizaciones automáticas e instalar las actualizaciones en Windows deberás acceder con permiso de administrador.

Actualización en Windows XP

Para indicarle al sistema que deseas utilizar el servicio de actualizaciones automáticas tendrás que pulsar con el botón derecho sobre **Mi PC**  seleccionar **Propiedades** ➔ pestaña **Actualizaciones automáticas**.

También puedes acceder a la misma ventana pulsando el icono de **Alertas de seguridad de Windows**  de la barra de tareas que abrirá el **Centro de Seguridad** ➔ **Actualizaciones automáticas**. En el Centro de seguridad encontrarás información del estado del Firewall, Actualizaciones y antivirus.



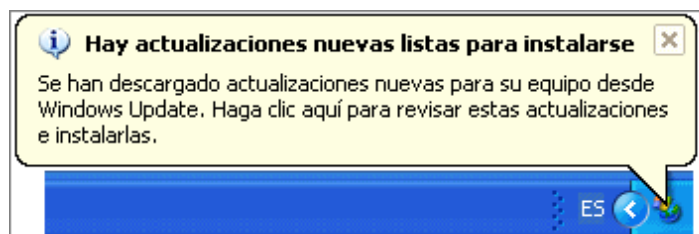
En la captura de pantalla que se muestra se ha optado por la opción de descarga e instalación automática que es la que por defecto recomienda el sistema. Se trata de la opción más conveniente para garantizar el correcto funcionamiento y seguridad de tu Windows.


La descarga se produce en segundo plano y la instalación se realizará antes de apagar el equipo, de forma que cuando vuelvas a arrancar ya tendrán efecto dichas actualizaciones.

En otros casos, dependiendo de la versión de Windows o de la configuración establecida, puede que sea justo tras la instalación de la actualización cuando se te pida que reinicies el sistema para que puedan tener efecto los cambios. En ese caso podrá optar por realizarlo en ese momento o retrasarlo a cuando vayas a apagar tu ordenador.

También, en esa misma opción, puedes elegir la frecuencia diaria y la hora de chequeo e instalación de las actualizaciones. Debes saber que si en esa frecuencia de fecha y hora no estuvieras conectado a Internet para poder realizar la actualización, entonces se realizará en la inmediata conexión siguiente que sí lo estuvieras.

Si seleccionas la segunda opción **Descargar actualizaciones por mí, pero permitirme elegir cuándo instalarlas**, las actualizaciones se descargan en segundo plano sin que te enteres y al concluir la descarga recibirás un aviso en la barra de tareas.




El aviso te informa de que existen nuevas actualizaciones listas para instalarse y podrás optar si quieres que se instalen o no en ese momento pulsando sobre el propio aviso. Tras la instalación de algunas de las actualizaciones descargadas puede que se requiera reiniciar el ordenador. Por ello, si prefieres no interrumpir el trabajo que estabas realizando puedes pulsar el botón **Recordármelo más tarde** .

La tercera opción, como indica su enunciado, **Notificarme, pero no descargarlas automáticamente ni instalarlas**, te permite sólo recibir información de que hay actualizaciones disponibles.

La última opción es **Desactivar Actualizaciones automáticas**, señalándote que de esa forma tu equipo es más vulnerable por no estar actualizado. Igualmente te muestra un enlace al **sitio Web de Windows Update** al que te podrás conectar para la descarga manual.

Independientemente de que tengas configurada una actualización automática sería conveniente que visitaras, de forma esporádica, la página de actualización manual puesto que puedes encontrar actualizaciones que, al no considerarse críticas, no se hayan obtenido mediante el servicio automático.

Para acceder a la a la página del **sitio Web de Windows Update** para la realización de una actualización manual podrás hacerlo pulsando con el botón derecho sobre **Mi PC**  ➡

seleccionar **Propiedades** ➡ pestaña **Actualizaciones automáticas** ➡ en el enlace **sitio Web de Windows Update** de la última opción de desactivación de Actualizaciones Automáticas. También puedes acceder a la misma dirección desde el propio navegador Internet Explorer mediante la opción de menú **Herramientas** ➡ **Windows Update**.

Aunque hayas decidido utilizar habitualmente otro navegador, si quieres acceder a la página de actualizaciones de Windows para utilizar el servicio deberás hacerlo, obligatoriamente, con Internet Explorer.

Es probable que, la primera vez que accedas al servicio, se produzca un primer paso en el que se solicitará tu permiso para instalar la última versión de las herramientas de gestión de las actualizaciones. Te resultará imprescindible conceder la autorización para poder continuar con el proceso. Una vez completada aparecerá una pantalla de bienvenida en la que solicitaremos que se busquen las actualizaciones disponibles.



Es requisito imprescindible el tener una copia original del sistema operativo Windows instalada en tu ordenador pues, como paso previo a la actualización, se comprobará la originalidad del Windows instalado y si no fuera correcto no se llevará a cabo la actualización.

Puedes escoger entre una actualización rápida y otra personalizada:

- La opción **Rápida** aparece como recomendada porque localizará las actualizaciones críticas. Se llama así a aquellas que se han diseñado para cubrir una vulnerabilidad en el sistema que puede comprometer la seguridad del mismo, permitiendo el acceso no autorizado mediante códigos malignos, parches que solucionan problemas críticos del equipo, entendiendo como tales aquellos que comprometen la seguridad del mismo y su vulnerabilidad ante ataques de terceros.

Una vez finalizado el análisis del equipo se muestran los resultados.

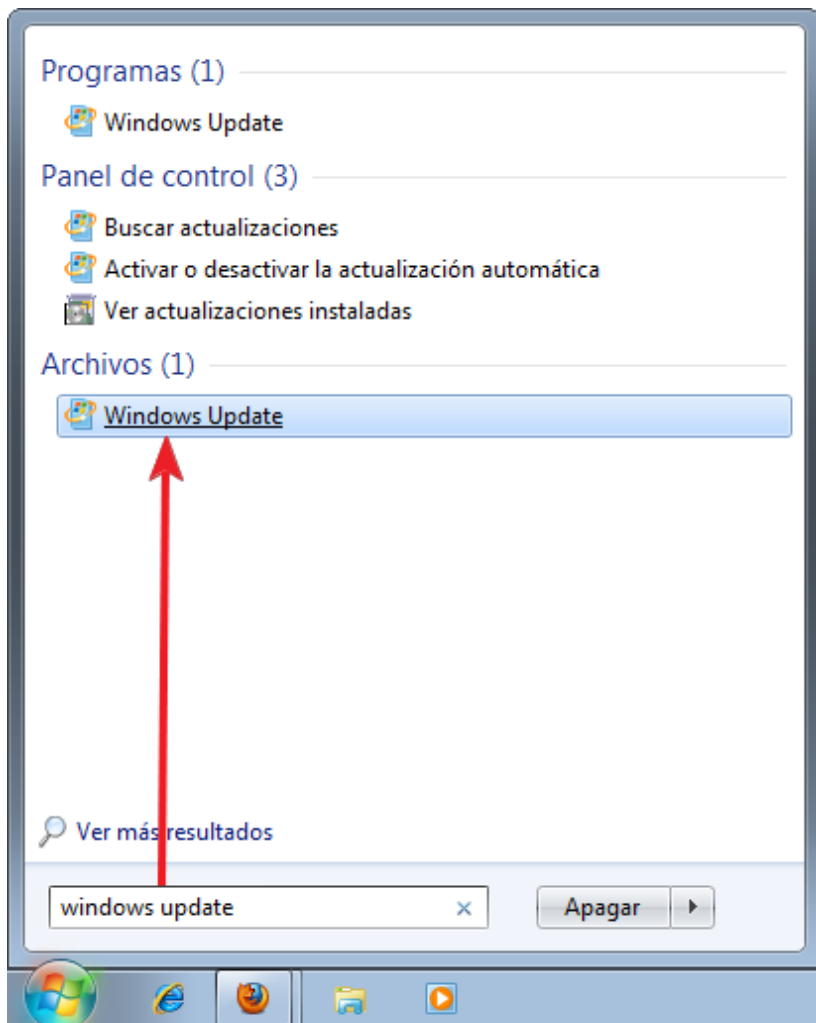
- La opción de **Personalizada** es más completa y permite la actualización del sistema Windows y también para todo el software y hardware de tu ordenador.

Tras seleccionar los componentes y pulsa Instalar se llevará a cabo el proceso de descarga e instalación y finalmente, dependiendo de los componentes seleccionados, es posible que se nos solicite confirmación para autorizar alguna operación y que el sistema tenga que reiniciarse para completar la instalación sustituyendo archivos que pudieran estar en uso por los recién descargados.

Actualización automática y manual en Windows 7

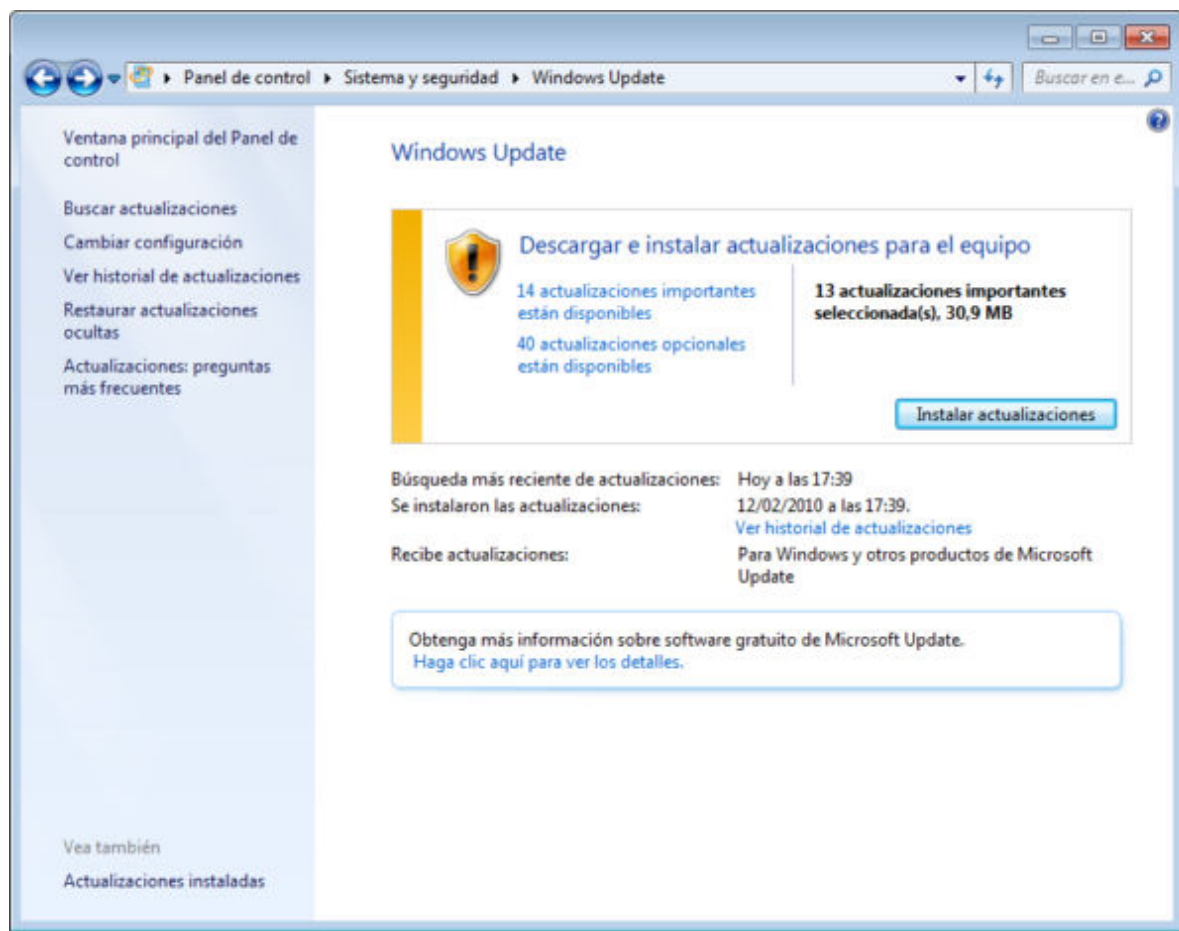
El funcionamiento de las actualizaciones en Windows 7 es muy parecido al comentado para Windows XP.

Para acceder a localizar Windows Update el modo más sencillo es desde **Inicio** ➡ **Buscar programas y archivos** escribiendo el nombre del programa Windows Update.



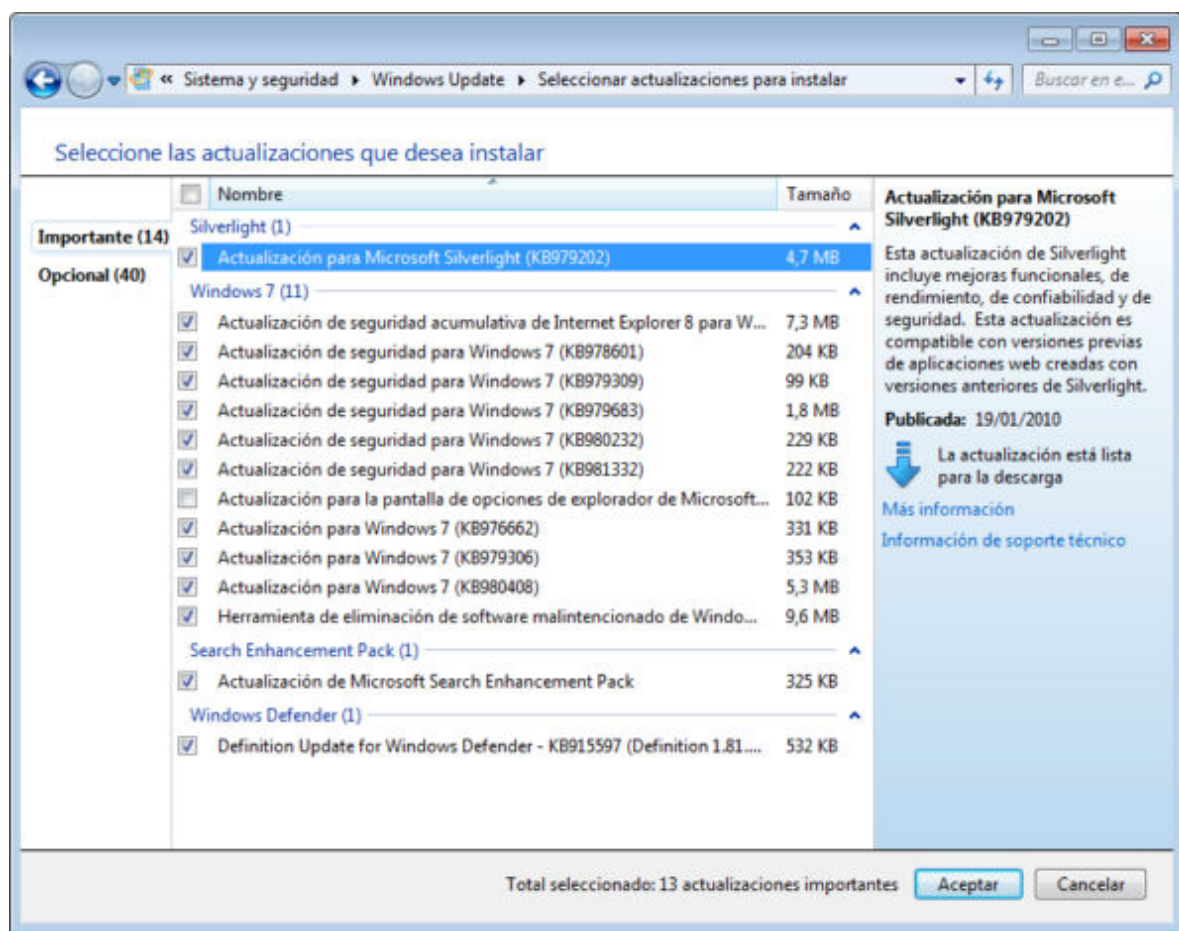
Tras pulsar sobre el programa localizado se abrirá la ventana de opciones de Windows Update que te presentará un resumen de la situación de las actualizaciones de tu equipo según la configuración que tengas establecida.

Como bien sabes, para algunas opciones y programas en Windows se pueden utilizar varios caminos para llegar al mismo sitio. En este caso si te fijas en la barra de dirección podrás comprobar que también podrías llegar a Windows Update desde **Inicio ➡ Panel de Control ➡ Sistema y Seguridad ➡ Windows Update**. Igualmente también podrías haber llegado desde los avisos y el icono del **Centro de actividades** de la barra de tareas.

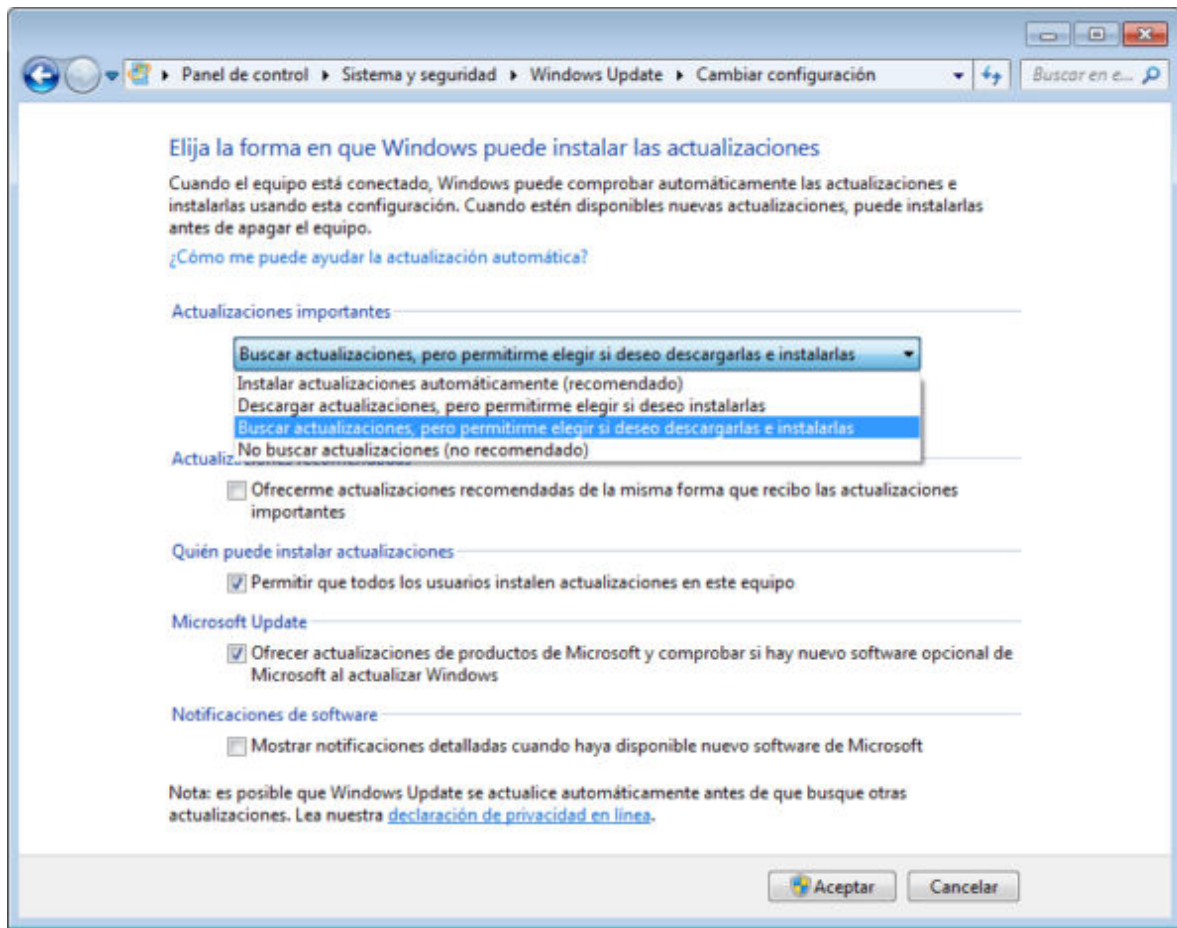


En la imagen que se muestra Windows nos informa y recomienda sobre diversas actualizaciones importantes y opcionales listas para si queremos instalarlas. También nos informa de cuándo se realizó la última actualización y nos permite ver el historial de dichas actualizaciones.

Si deseamos ver las **actualizaciones disponibles** pulsáramos sobre esas indicaciones y se nos abrirá una nueva ventana para que elegir aquellas que deseamos instala tanto de las importantes y como de las opcionales y cuando las tengamos elegidas al pulsar Aceptar volveremos a la pantalla inicial para, si lo deseamos, proceder a la instalación de las escogidas.



Si pulsamos la opción de **Cambiar la configuración** que figura en el marco izquierdo de opciones, podrás comprobar que la configuración de estado presentada en la pantalla principal se debe a que la configuración de nuestro equipo está en modo **Buscar actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas**.



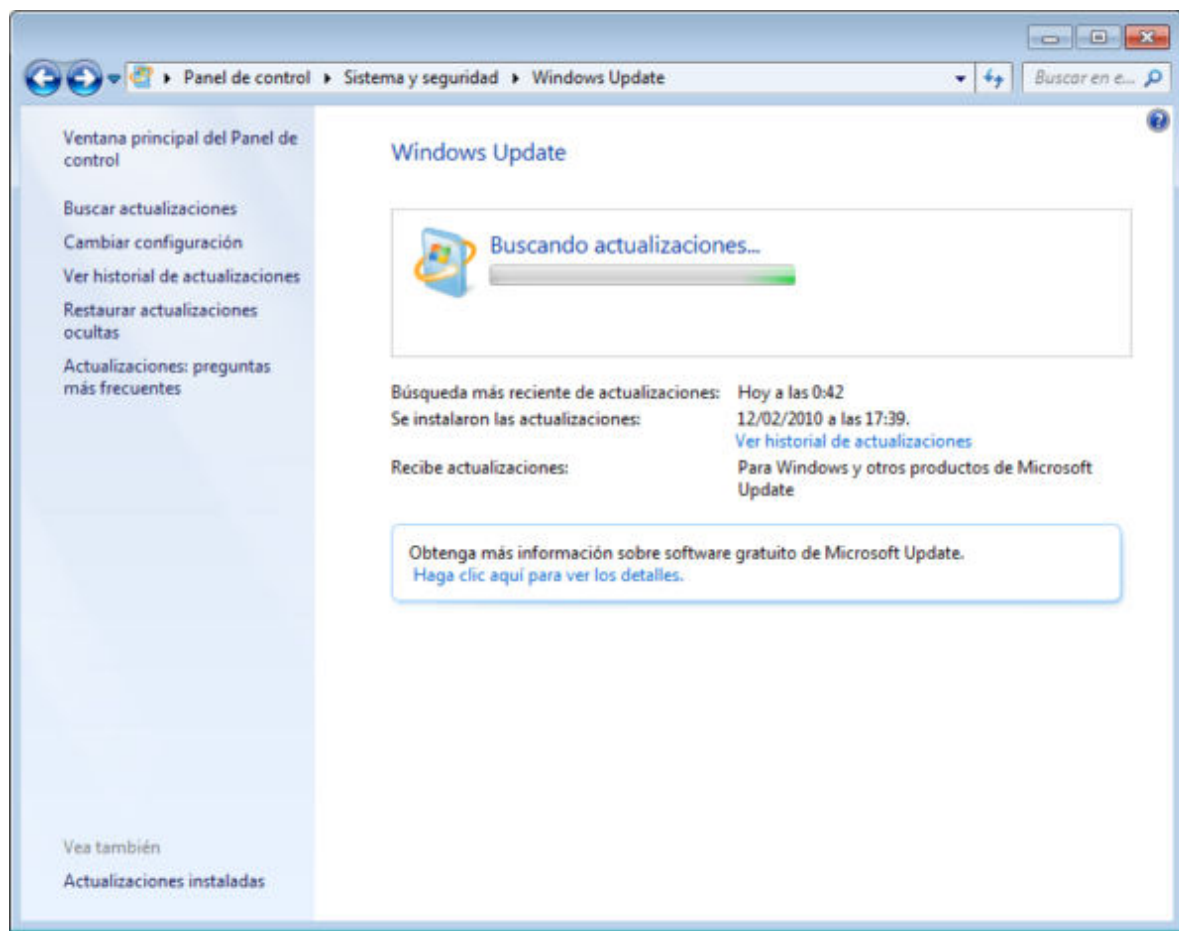
Windows 7 posee las mismas opciones de actualizaciones que Windows XP:

1. **Instalar actualizaciones automáticamente** (recomendado por el propio Windows).
2. **Descargar actualizaciones**, pero permítirme elegir si deseo instalarlas.
3. **Buscar actualizaciones**, pero permítirme elegir si deseo descargarlas e instalarlas.
4. **No buscar actualizaciones** (no recomendado por Windows).

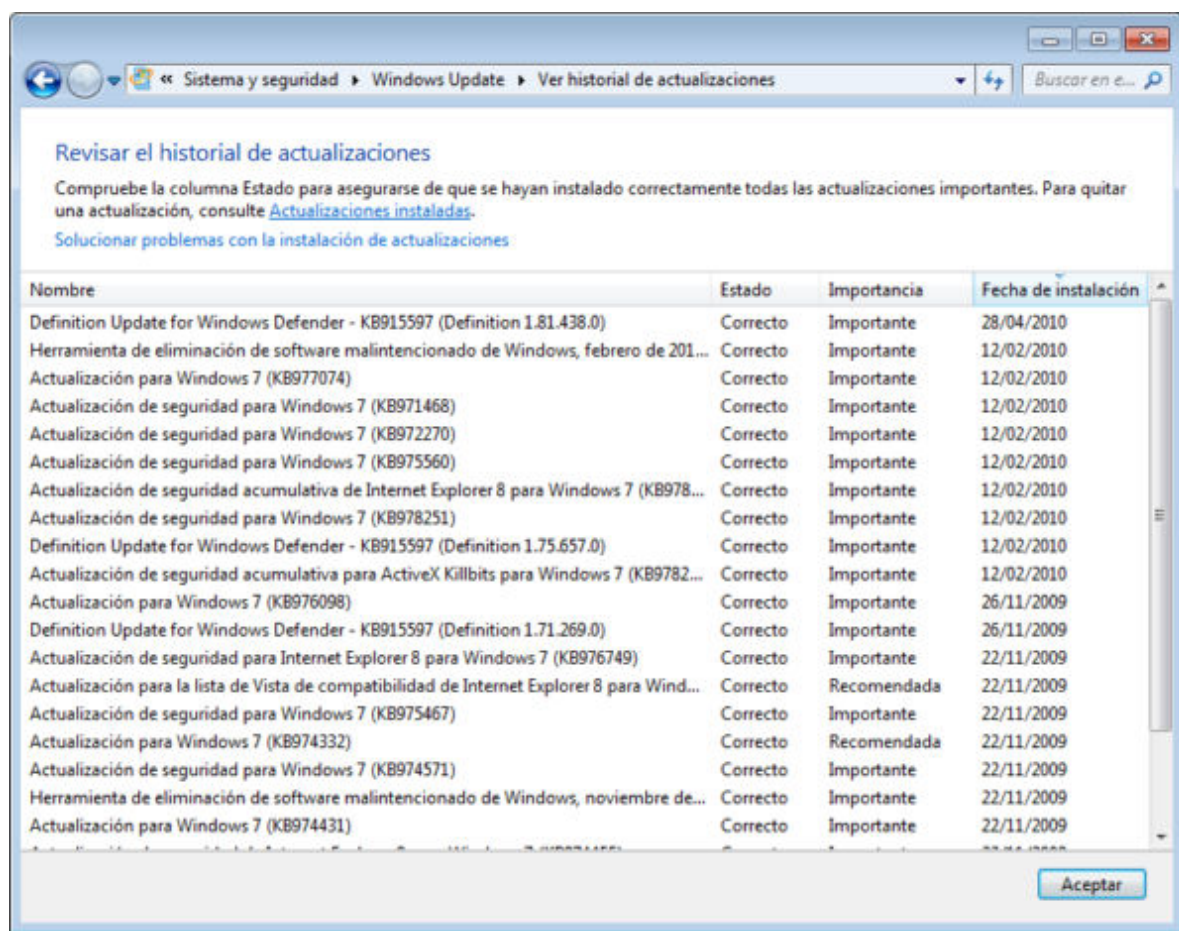
Igualmente en estas opciones de instalación de actualizaciones puedes seleccionar si deseas recibir actualizaciones recomendadas, permitir a otros usuarios la instalación y las notificaciones de nuevo software.

El resto de opciones de Windows Update tienen una funcionalidad claramente expresada en su propio enunciado.

Buscar actualizaciones, te permite la búsqueda de actualizaciones pero que no se instalarán. La instalación siempre dependerá de la opción elegida en la forma en que Windows puede instalar las actualizaciones.



Ver el historial de actualizaciones te permite revisar las actualizaciones instaladas mostrándote el nombre, estado de instalación, la importancia y la fecha en que se llevó a cabo dicha instalación.



También podemos restaurar actualizaciones ocultas anteriormente y finalmente, tras concluir la instalación, es posible que se solicite reiniciar el sistema para que tengan efecto las actualizaciones o que si éstas no son muy importantes se acaben de instalar al ir a apagar el ordenador.

Como puedes observar el funcionamiento de Windows Update es muy sencillo, pero de su correcta operatividad y de su actualización frecuente dependerá el buen funcionamiento de tu sistema operativo.

Recuerda que tu sistema operativo es la base en la que se sustentan el resto de los programas y aplicaciones instaladas en tu ordenador. La actualización es una puesta al día que te posibilita múltiples ventajas sobre todo en temas de seguridad y resolución de problemas críticos que se pudieran presentar.

Publicar en Internet

Todo contenido (texto, ficheros, fotos, video,...) que está en Internet ha sido colocado por alguien, por lo tanto tiene dueño. Muchos de estos contenidos, objetos digitales, obras y creaciones están referenciados con su autoría e incluso la licencia de uso que tienen, suele pasar mucho en los vídeos, fotografías, imágenes, obras literarias, documentación, apuntes, manuales, obras literarias,....





También puedes encontrar que muchos contenidos e información de Internet no tengan ninguna referencia a su titularidad, pero el hecho de que no aparezca la autoría o que no se explicita el uso permisivo o restrictivo que poseen dichos contenidos, no significa que puedas copiarlos y utilizarlos libremente como te venga en gana.

Desde el momento de su creación toda obra tiene un reconocimiento legal de autoría. Es precisamente ese reconocimiento legal que se dan a todos los contenidos, lo que nos permite también a nosotros tener la tranquilidad de poder publicar nuestras propias creaciones originales (vídeos, fotos, textos, apuntes, etc.) sabiendo que pueden estar salvaguardados de un uso inadecuado.

Así pues, todo contenido tiene unos derechos de autor y depende del propio autor el determinar el uso y distribución que se pueda hacer de su obra. En este sentido podríamos esquematizar los tipos de licencias de contenidos en Internet del siguiente modo:

- **© Copyright:** es un tipo de licencia general y básica muy extendida en el mundo editorial y audiovisual. Tiene un carácter más restrictivo y suele conllevar todos los derechos reservados.
- **CC Creative Commons:** normalmente indicado como las letras CC. Las obras CC también tienen copyright de reconocimiento de autoría, aunque se caracterizan por que permite copiarlas y distribuirlas. El modo de distribución obras se explicitan en cada uno de los tipos de licencias Creative Commons.







Las licencias Creative Commons se basa en cuatro condicionantes:

	Reconocimiento (Attribution): En cualquier explotación de la obra autorizada por la licencia hará falta reconocer la autoría.
	No Comercial (Non commercial): La explotación de la obra queda limitada a usos no comerciales.
	Sin obras derivadas (No Derivate Works): La autorización para explotar la obra no incluye la transformación para crear una obra derivada.
	Compartir Igual (Share alike): La explotación autorizada incluye la creación de obras derivadas siempre que mantengan la misma licencia al ser divulgadas.



Los cuatro condicionantes anteriores dan lugar a seis tipos de licencias Creative

Commons:

	Reconocimiento (by): Se permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación de obras derivadas, la distribución de las cuales también está permitida sin ninguna restricción.
	Reconocimiento - NoComercial (by-nc): Se permite la generación de obras derivadas siempre que no se haga un uso comercial. Tampoco se puede utilizar la obra original con finalidades comerciales.
	Reconocimiento - NoComercial - CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.
	Reconocimiento - NoComercial - SinObrasDerivadas (by-nc-nd): No se permite un uso comercial de la obra original ni la generación de obras derivadas.
	Reconocimiento - CompartirIgual (by-sa): Se permite el uso comercial de la obra y de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.
	Reconocimiento - SinObrasDerivadas (by-nd): Se permite el uso comercial de la obra pero no la generación de obras derivadas.



licencia Creative Commons

Para usar una obra Creative Commons no necesitas pedir permiso al autor, así es muy fácil utilizarla. Sólo tendrás que ceñirte al tipo de uso y podrás copiarla y utilizarla.

Puedes ver un simpático vídeo explicativo de [qué son las licencias Creative Commons](#) colocado en Youtube.

Cuando un contenido de Internet pueda serte interesante para tu labor docente es bueno localizar la autoría y la licencia que sobre dicho contenido ha realizado el autor, de ese modo sabrás que tipo de utilización te está permitido realizar.

Es cierto que muchos de los contenidos que existen en Internet no poseen una identificación de autoría, así que la primera consideración que te hacemos es que tú en tus publicaciones en Internet lo hagas.

También te damos unos consejos:

1. Siempre que sea posible, deberás **ponerte en contacto con el autor para solicitarle la autorización** y comentarle el uso que piensas hacer de su obra, ya sea total o parcialmente.

2. Si no hay ningún interés comercial y no se expresa la autoría, es norma de educación **citar la fuente** de dónde fue tomada.
3. Es importante **ser dueños o poseedores de los derechos de la información que colocamos en Internet**.
4. **Derechos del menor:** Dado que estamos en un ámbito educativo, es necesario señalar el cuidado que se debe de tener en el tratamiento de **datos de carácter sensible y los derechos de imagen del menor**.

Siempre que publiquemos alguna **imagen de menores en Internet tenemos que tener la autorización firmada de sus padres o tutores**. Así es una buena medida que todo centro educativo posea un formulario donde los padres o tutores autoricen o denieguen de forma expresa el uso de imágenes o material audiovisual de sus hijos en Internet y que esa autorización forme parte del expediente del alumno mientras permanezca en el centro.

Ya sabes que por el hecho de estar publicado un contenido en Internet no implica que sea de dominio público y lo puedas copiar. La autorización del autor siempre que sea posible has de tenerla. En la mayoría de los casos es un trámite que agradece el autor y una forma de reconocer su trabajo.

Si la utilidad que quieres dar al contenido que te gusta de Internet es para ponerlo también en Internet, puedes hacerlo **respetando la legalidad** simplemente **enlazándolo o**, si hay posibilidad, **incrustándolo en tu propio sitio web**. Cuando enlazamos o incrustamos un contenido en un blog, wiki, página web, etc. no incumplimos ninguna ilegalidad pues estamos respetando el contenido original del autor en su propia web (con el enlace) o visualizándolo incrustado en la nuestra. Esta última posibilidad es la que te ofrecen la mayoría de los recursos de la web 2.0 al darte el código html del objeto para que lo puedas pegar en tu página web y así parezca parte de tu contenido.

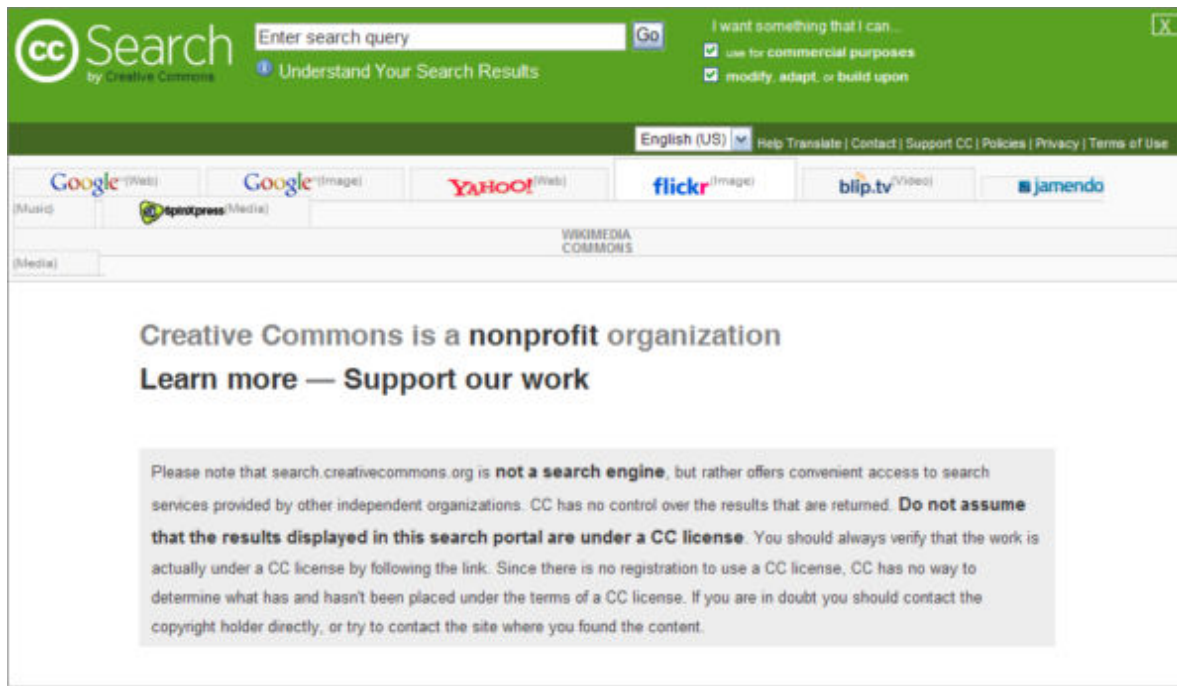
La utilización sin permiso de un contenido de Internet para un uso educativo, aunque no lucrativo o tenga uso comercial, puede ser un atenuante de la infracción pero nunca un eximente de la obligatoriedad de cumplir con la ley.

Los contenidos de pago suelen estar bastante claros, así que no les dedicaremos ninguna mención especial.

Sobre los recursos libres y gratuitos que podemos utilizar, decirte que hay infinidad de ellos en Internet y que sólo tendrás que buscar un poco para encontrar lo que necesitas. En esta misma documentación has podido conocer aplicaciones y programas comerciales y otros muchos gratuitos que son una muestra de la gran diversidad de opciones existentes en Internet.

Relacionado con el mundo educativo y universitario existe un movimiento global de usuarios de Internet con una filosofía de cooperación y colaboración solidaria. Fácilmente podrás encontrar ayuda y recursos aportados por otros internautas de modo desinteresado.

Creative Commons pone a disposición de todos los usuarios **CC Search**, un servicio de búsqueda de recursos bajo licencia Creative Commons que utilizando los motores de búsqueda de otras empresas como Google, Yahoo, etc. que facilita su localización.



1. La **seguridad**: debes de preservar la seguridad de tu ordenador así que ten cuidado con todo aquello que te bajas e instalas. Busca sitios de garantía, te asegurarás que están libres de virus y que se corresponden con lo que verdaderamente anuncian. Hay bastante sitios web de contrastada trayectoria como para fiarte de lo que te ofrecen: [softonic](#), [tucows](#), etc.
2. La **licencia de uso** que otorgan: respecto al uso puedes diferenciar entre:
 1. **Software propietario**: son programas comerciales de pago.
 2. **Software demo (trial)**: programas comerciales con una licencia temporal. Pueden tener también limitadas algunas de las funcionalidades del programa completo. Caducan después del período de prueba.
 3. **Software gratuito (free)**: son programas no comerciales, libres y gratis para su uso, no hay que pagar por ellos. En el software gratuito hay todo un abanico de posibilidades y matices entre ellos: freeware, de dominio público, Open Source, licencias GPL o copyleft, etc. En algunos casos puedes encontrarte con mensajes que te solicitan una donación voluntaria.
 4. **Shareware**: son programas gratis durante un tiempo, después pueden dejar de funcionar o te requerirte insistentemente una pequeña aportación para seguir funcionando.
 5. **Software pirata o warez**: son programas ilegales. Se trata de software comercial al que se le ha vulnerado la licencia de uso, como por ejemplo pirateando su número de registro.

Puedes consultar más información en Wikipedia sobre el [software libre](#) y el [software propietario](#).



Actividad 1

Localiza en la página de alguna empresa antivirus la "ficha técnica" de cuatro virus informáticos recientes, especificando su nombre, daño potencial, manera de manifestarse y propagarse. Averigua también a qué nos referimos cuando se habla de "phising" y la forma de protegerte de este tipo de ataque.
