



GUIA ILUSTRADA: **McAfee Multi Dispositivos de Tigo y McAfee** **Pc Windows**

Contenido:

1.	Panel inicio McAfee:.....	<u>4</u>
1.1	Descripción Panel de Inicio	<u>5</u>
1.1.1	Protección Antispyware y Antivirus:	<u>6</u>
1.1.1.1	Análisis de su PC:	<u>7</u>
1.1.1.1.1	Análisis rápido:	<u>8</u>
1.1.1.1.2	Análisis completo	<u>9</u>
1.1.1.1.3	Análisis personalizado	<u>10</u>
1.1.1.1.4	Análisis manual	<u>11</u>
1.1.1.1.5	Visualización del proceso de análisis:	<u>11</u>
1.1.1.2	Análisis en tiempo real:	<u>13</u>
1.1.1.2.1	Configuración:	<u>15</u>
1.1.1.2.2	Configuración de inicio:	<u>16</u>
1.1.1.2.3	Excluir archivos	<u>16</u>
1.1.1.3	Análisis planificado	<u>19</u>
1.1.1.3.1	Planificación del análisis personalizado	<u>20</u>
1.1.1.3.2	Archivos y carpetas excluidas:	<u>22</u>
1.1.2	Protección del correo electrónico y la web	<u>24</u>
1.1.2.1	Firewall:	<u>25</u>
1.1.2.1.1	Desactivar:	<u>26</u>
1.1.2.1.2	Controlador de tráfico	<u>28</u>
1.1.2.1.3	Consejo inteligente y configuración avanzada	<u>28</u>
1.1.2.1.4	Historial de firewall	<u>19</u>
1.1.2.1.5	Conexiones a internet para programas	<u>30</u>
1.1.2.1.6	Mis conexiones de red	<u>31</u>
1.1.2.1.7	Puertos y servicios del sistema	<u>31</u>
1.1.2.1.8	Protección de intrusiones	<u>32</u>
1.1.2.1.9	NetGuard.....	<u>32</u>
1.1.2.2	AntiSpam.....	<u>33</u>
1.1.2.2.1	Niveles de protección Anti-Spam	<u>34</u>



1.1.2.2.2	Procesamiento de correos electrónicos	<u>34</u>
1.1.2.2.3	Barra de herramientas Anti-Spam.....	<u>34</u>
1.1.2.2.4	Reglas de filtrado personalizadas	<u>35</u>
1.1.2.2.5	Lista de amigos	<u>35</u>
1.1.2.2.6	Conjunto de caracteres	<u>35</u>
1.1.2.2.7	Reglas de filtrado de WebMail	<u>36</u>
1.1.2.2.8	WebMail filtrado	<u>36</u>
1.1.2.3	SiteAdvisor	<u>37</u>
1.1.3	Actualizaciones de McAfee	<u>39</u>
1.1.3.1	Buscar actualizaciones	<u>40</u>
1.1.3.2	Actualizar configuraciones	<u>41</u>
1.1.4	Su suscripción	<u>42</u>
1.1.5	Protección de datos	<u>43</u>
1.1.5.1	FileLock.....	<u>44</u>
1.1.5.2	Shredder	<u>45</u>
1.1.6	Herramientas de red doméstica y equipo.....	<u>46</u>
1.1.6.1	Mi red doméstica.....	<u>47</u>
1.1.6.2	QuickClean.....	<u>47</u>
1.1.6.2.1	Configuración	<u>48</u>
1.1.6.2.2	Planificación	<u>48</u>
1.1.6.2.3	Analizador de vulnerabilidades	<u>49</u>
1.1.7	Control parental.....	<u>50</u>
1.1.7.1	Configuración de Control parental.....	<u>51</u>
1.1.7.1.1	Definir contraseña de administrador	<u>52</u>
1.1.7.1.2	Protección de los usuarios:	<u>54</u>
1.1.7.1.3	Definir una categoría de contenido como autorizada	<u>56</u>
1.1.7.1.4	Uso de la búsqueda segura	<u>57</u>
1.1.7.1.5	Autorizar y bloquear sitios web	<u>58</u>
1.1.7.1.6	Control del tiempo de navegación en la web.....	<u>60</u>
2.	Centro de navegación	<u>62</u>
2.1	Configuración	<u>63</u>
2.1.1	Suscripción.....	<u>63</u>
2.1.2	Alertas y configuraciones generales	<u>64</u>
2.1.2.1	Configuración general	<u>64</u>



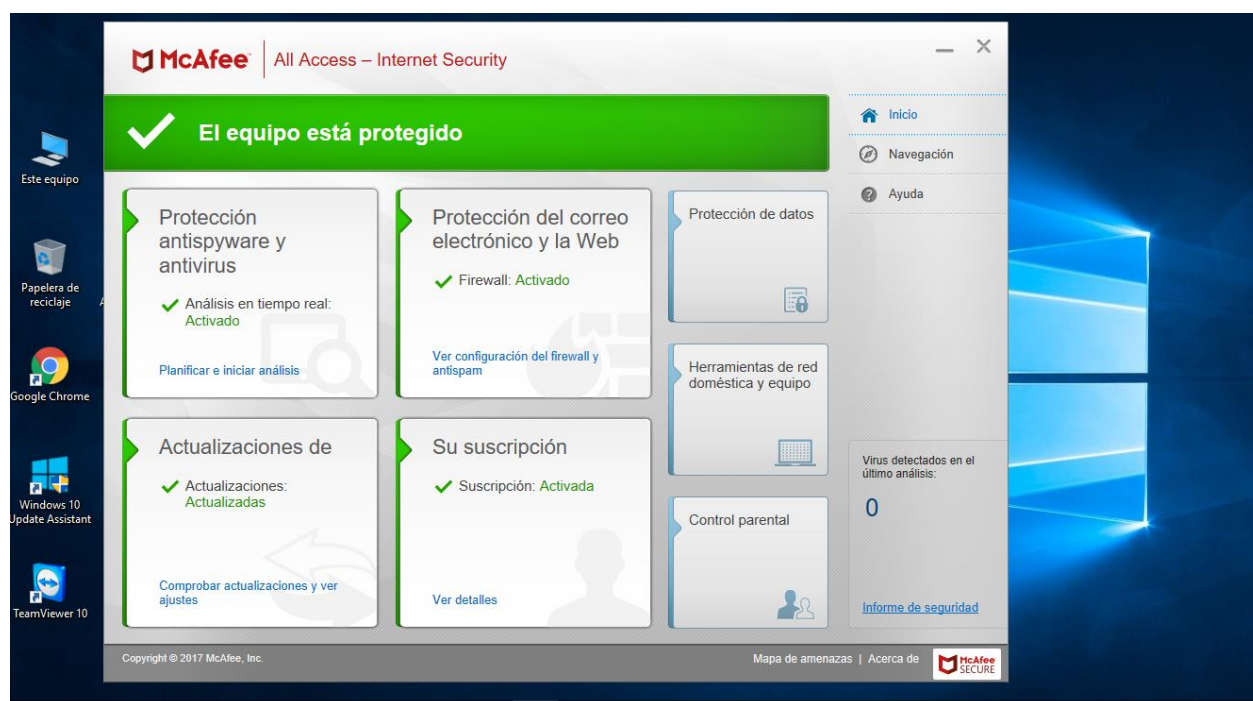
2.1.2.2	Alertas informativas.....	<u>65</u>
2.1.2.3	Alertas de protección	<u>65</u>
2.1.2.4	Protección de acceso	<u>65</u>
2.1.3	Funciones.....	<u>66</u>
2.2	Informes e historial	<u>67</u>
2.2.1	Informe de seguridad	<u>67</u>
2.2.2	Control parental.....	<u>69</u>
2.2.3	Historial de seguridad	<u>71</u>
3	Recursos de McAfee	<u>72</u>
3.1	Ayuda y soporte	<u>72</u>
3.2	Mapa de amenazas.....	<u>73</u>
3.3	Virus information library.....	<u>73</u>
3.4	HackerWatch.....	<u>73</u>
3.5	Acerca de	<u>74</u>

Esta guía ilustrada está basada en la consola de McAfee Multi Access – Internet Security **Versión 14.0** para consultar la versión de su consola ingrese a la sección **“Centro de navegación” “recurso de McAfee” “Acerca de”**

1. Panel inicio McAfee:

El panel de inicio de McAfee le permite comprobar rápidamente si el equipo está protegido y reparar los problemas de seguridad relacionados con el software de McAfee. Al abrir el panel de inicio, se puede saber al instante si la suscripción, el software y las funciones de McAfee están actualizadas y funcionan correctamente.

Para acceder al panel de inicio, ingrese al icono de McAfee que hay en su escritorio:



O simplemente desde el icono de McAfee en la bandeja de sistema, con dos clics:



1.1 Descripción del panel de inicio

Permite visualizar su consola y dirigirse al campo que desee.

El panel de inicio controla la protección de su equipo para que permanezca protegido con las actualizaciones automáticas, administre su suscripción de McAfee y acceda a las funciones de protección y la configuración.

El panel de inicio de McAfee le permite comprobar rápidamente si el equipo está protegido y repara los problemas de seguridad relacionados con el software de McAfee. Al abrir la consola de inicio, puede saber al instante si la suscripción, el software y/o las características del producto están actualizadas y funcionan correctamente.



Esta guía ilustrada está basada en la consola de McAfee Multi Access – Internet Security **Versión 14.0** para consultar la versión de su consola ingrese a la sección **“Centro de navegación” “recurso de McAfee” “Acerca de”**

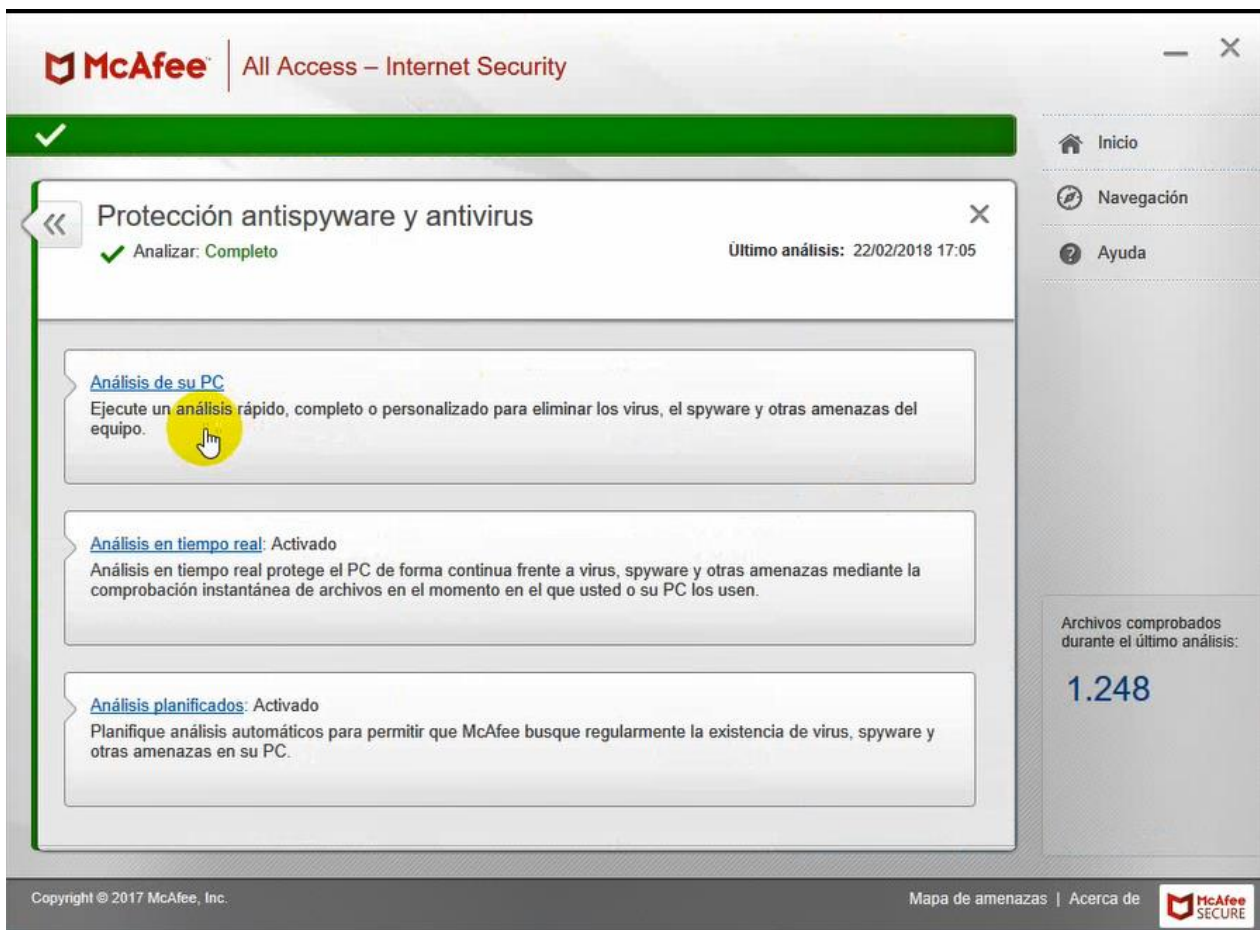
1.1.1 Protección Anti-Spyware y Anti-Virus McAfee:

El componente Anti-Spyware Anti-Virus de McAfee es la primera línea defensiva frente las amenazas de infección de virus, troyanos, gusanos, spyware y programas potencialmente no deseados, capturándolos en puntos de acceso como el correo electrónico, las unidades externas y las páginas Web.



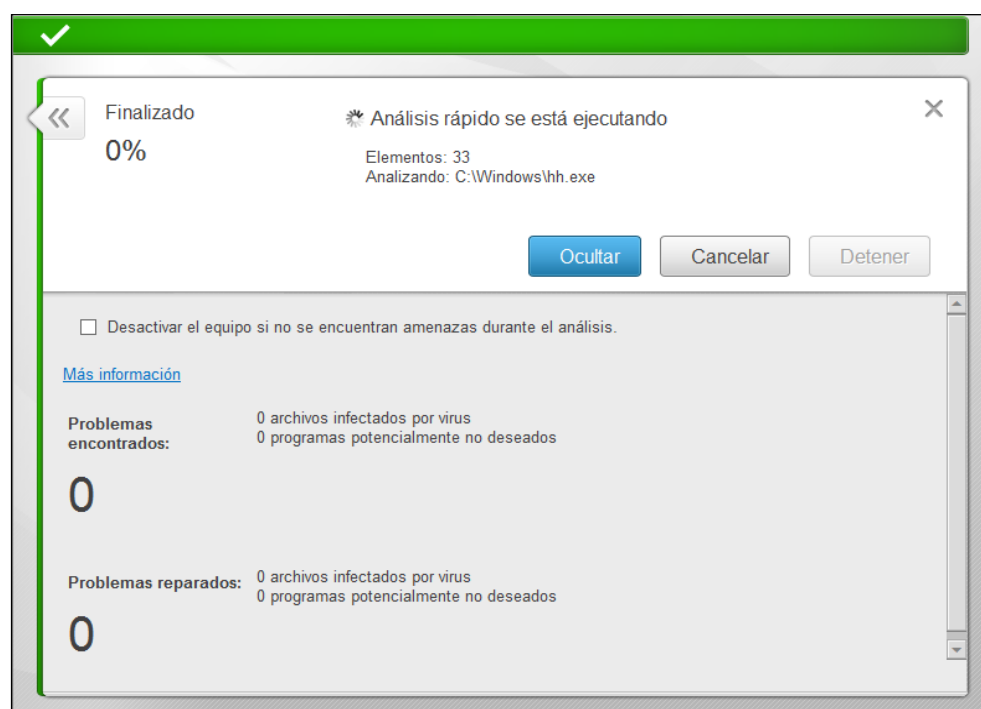
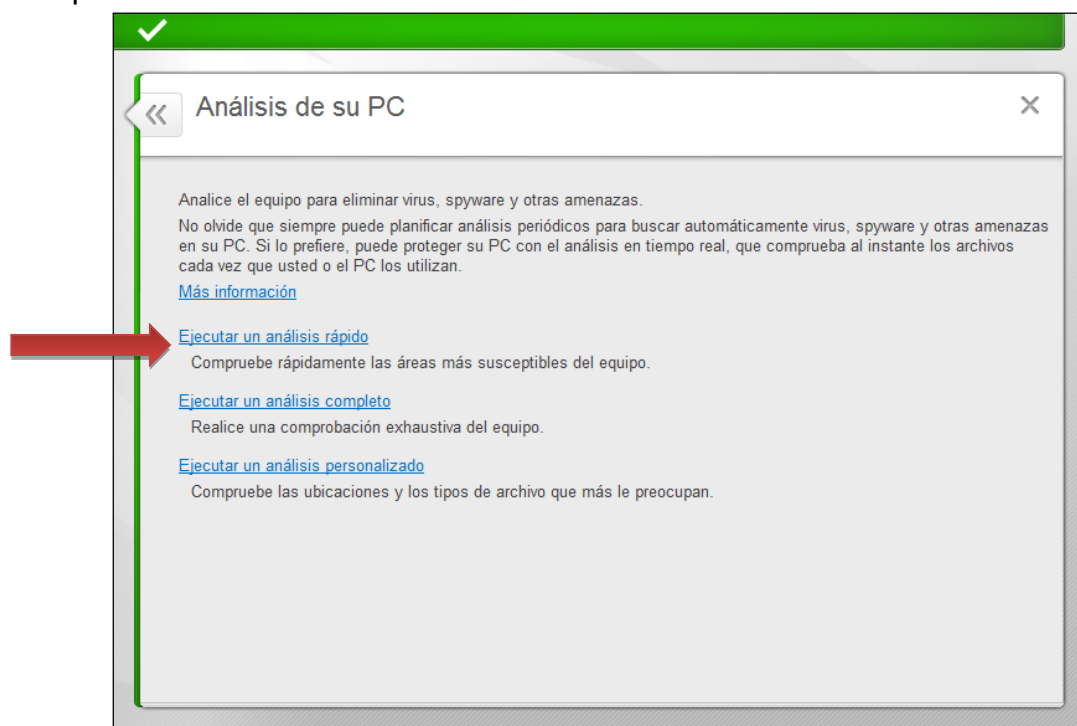
1.1.1.1 Análisis de su PC:

En función de sus necesidades de seguridad, puede elegir entre muchas opciones de análisis en Anti-Virus y Anti-Spyware, incluidos el análisis rápido, el análisis completo, el análisis personalizado y análisis manual. El tipo de análisis se selecciona en el Panel de inicio de McAfee, *Protección de antispyware y antivirus*, exceptuando el análisis manual. Para acceder a la configuración desde el panel de inicio, ingrese a *Protección de antispyware y antivirus*, luego *Análisis de su PC*



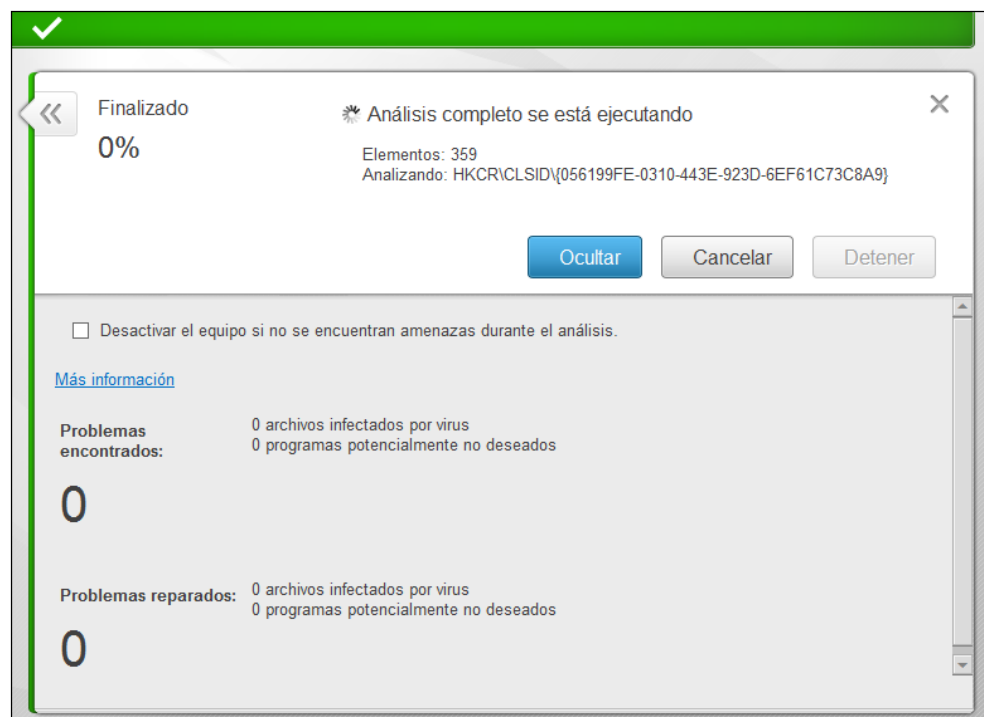
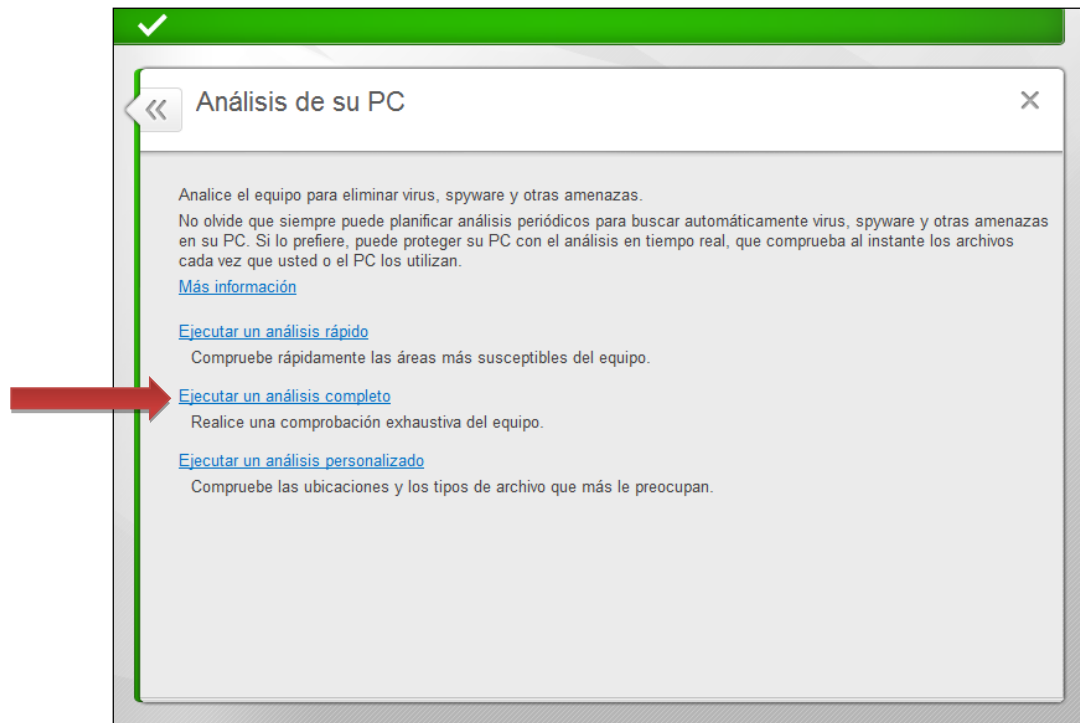
1.1.1.1.1 Análisis rápido:

Este tipo de análisis permite verificar rápidamente las áreas más vulnerables de su computador.



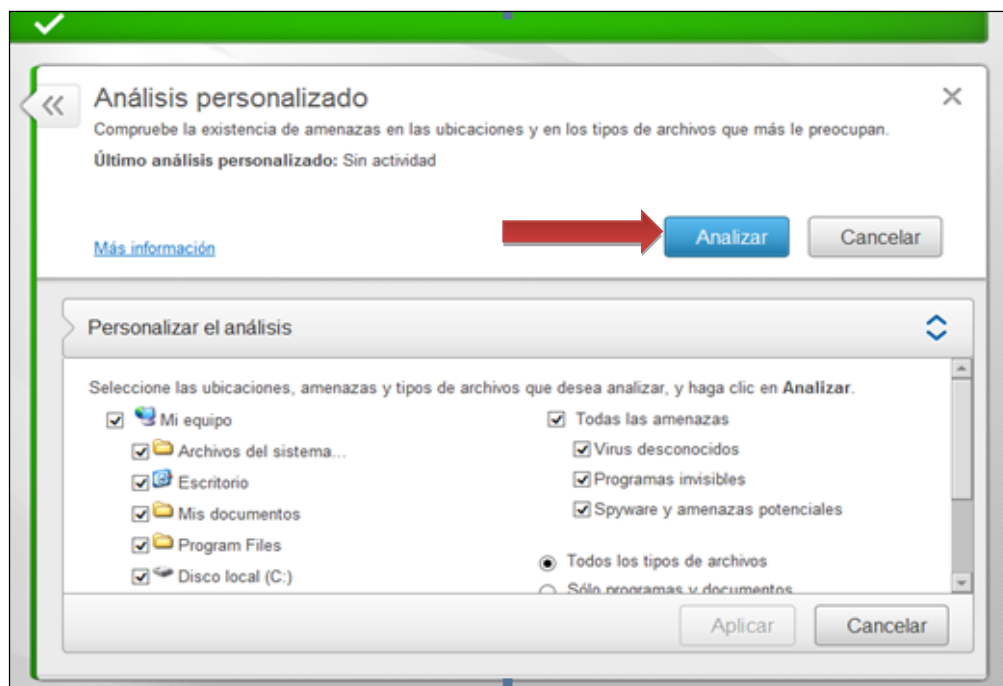
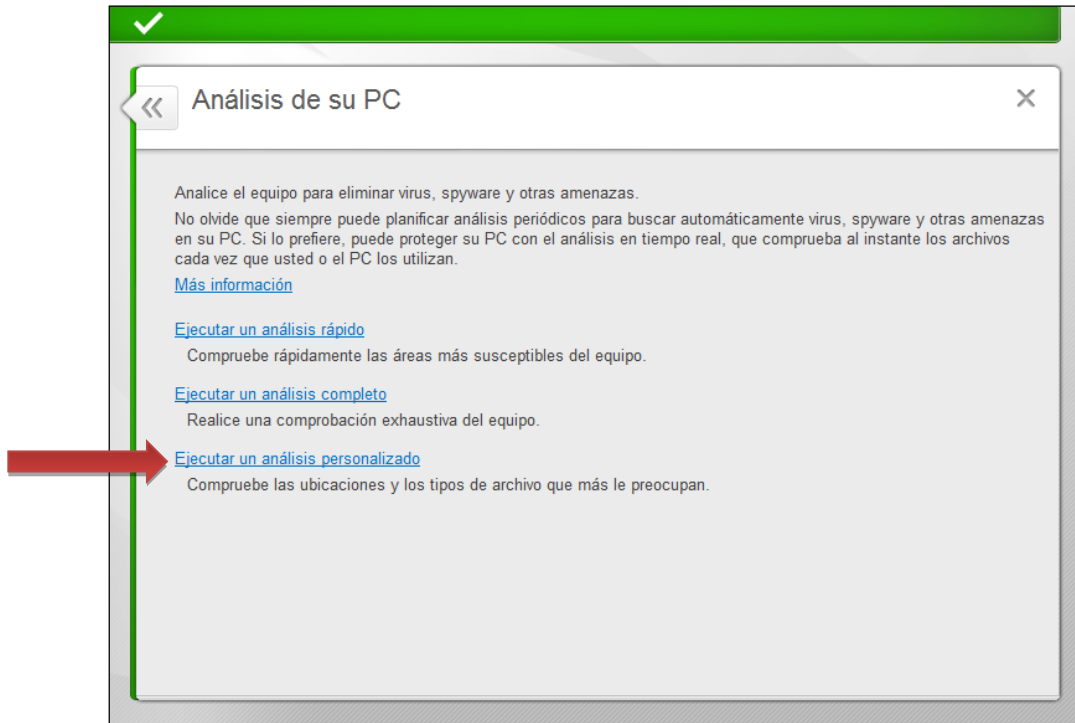
1.1.1.1.2 Análisis completo

Este tipo de análisis permite verificar de forma minuciosa todas las áreas de su computador.



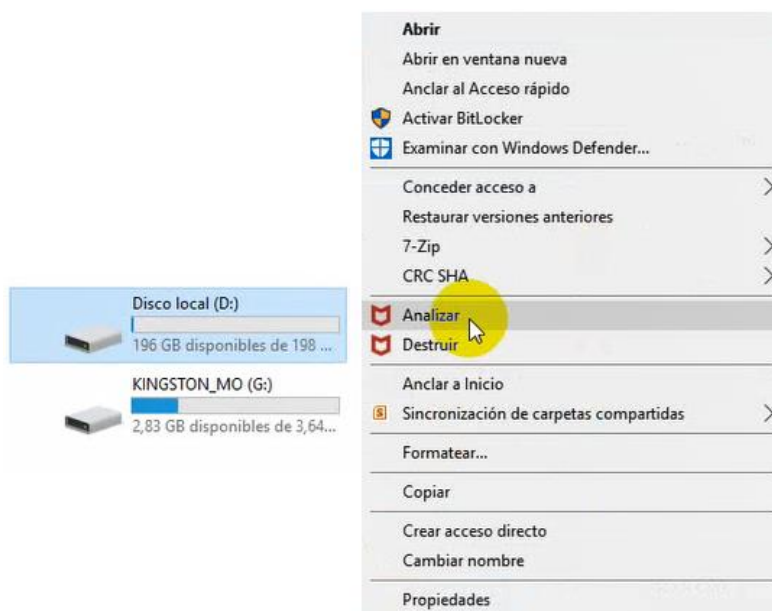
1.1.1.1.3 Análisis personalizado:

Este tipo de análisis permite escoger las áreas específicas que serán analizadas, junto con otras opciones:



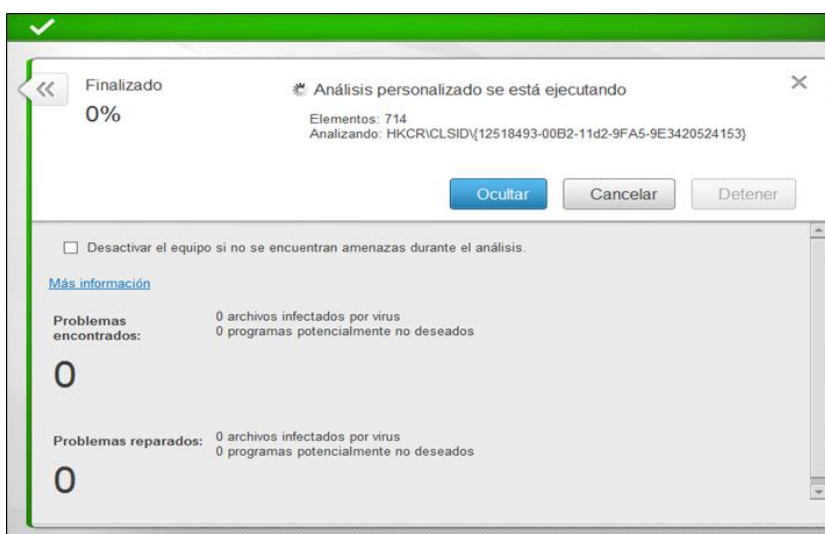
1.1.1.1.4 Análisis manual:

Aunque este tipo de análisis no se encuentra dentro del panel Análisis de su PC, se encuentra presente en el menú contextual de Windows, es decir, el menú desplegable que se visualiza cuando hacemos clic en el botón secundario del ratón. Esta opción es ideal para analizar unidades extraíbles o verificar archivos de forma individual

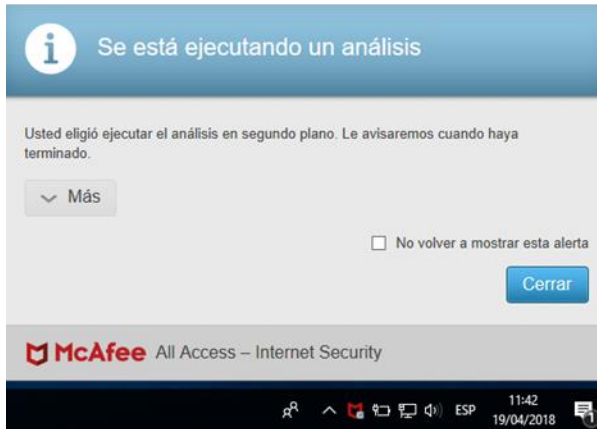


1.1.1.1.5 Visualización del progreso del análisis:

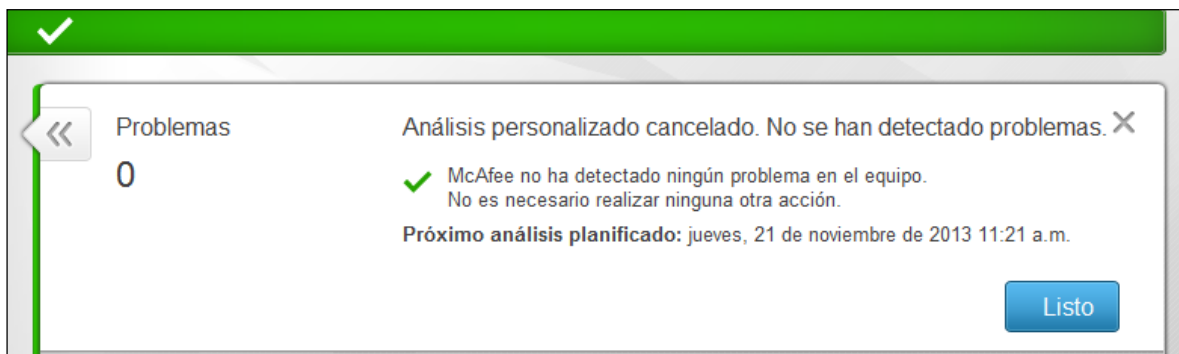
Cuando ejecuta un análisis, puede observar su progreso inmediatamente. McAfee muestra de forma simultánea los problemas que encuentra y los que repara. Entre estos problemas se encuentran archivos infectados por virus, programas potencialmente no deseados y cookies de rastreo. Si quedan problemas sin reparar una vez finalizado el análisis, McAfee le solicita que seleccione ciertas opciones para resolverlos. Adicionalmente tenemos las siguientes opciones.



Análisis en segundo plano. Esta opción nos permite minimizar la ventana del análisis en progreso, a la bandeja de sistema



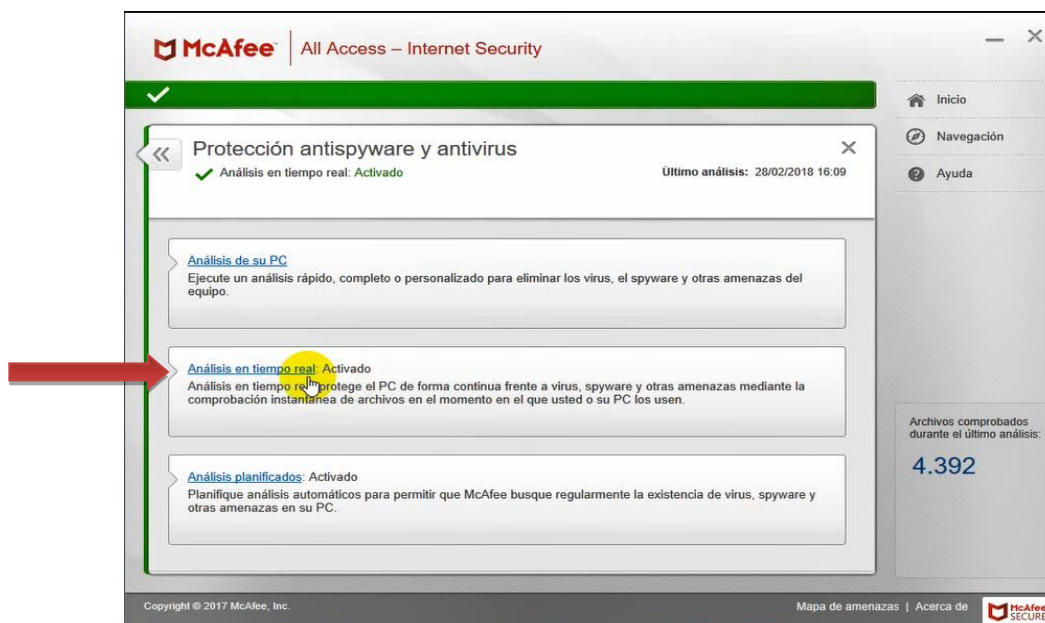
- *Detener:* Interrumpe el análisis para reanudarlo más tarde.
- *Reanudar:* Esta opción solo se activa cuando se detiene un análisis en progreso. Nos permite continuar con el análisis del computador.
- *Omitir:* Se pasa por alto un archivo que se está analizando actualmente, para pasar al siguiente archivo. Es recomendable cuando se trata de un archivo del cual se tiene absoluta confianza.
- *Cancelar:* Si se cancela parte del análisis, McAfee no puede detectar ningún otro problema hasta que ejecute el próximo análisis completo. Es aconsejable que finalice los análisis para detectar todas las amenazas potenciales.



McAfee puede apagar el equipo de forma automática tras comprobarlo en busca de amenazas. Al inicio del análisis en la página de progreso, seleccione Desactivar el equipo si no detecta amenazas durante el análisis.

1.1.1.2 Análisis en tiempo real:

Los análisis en tiempo real comprueban los archivos en busca de virus cada vez que usted o el equipo acceden a ellos. Para acceder a su configuración, ingrese desde el Panel de inicio a *Protección de antispyware y antivirus*, luego *Análisis en tiempo real*.

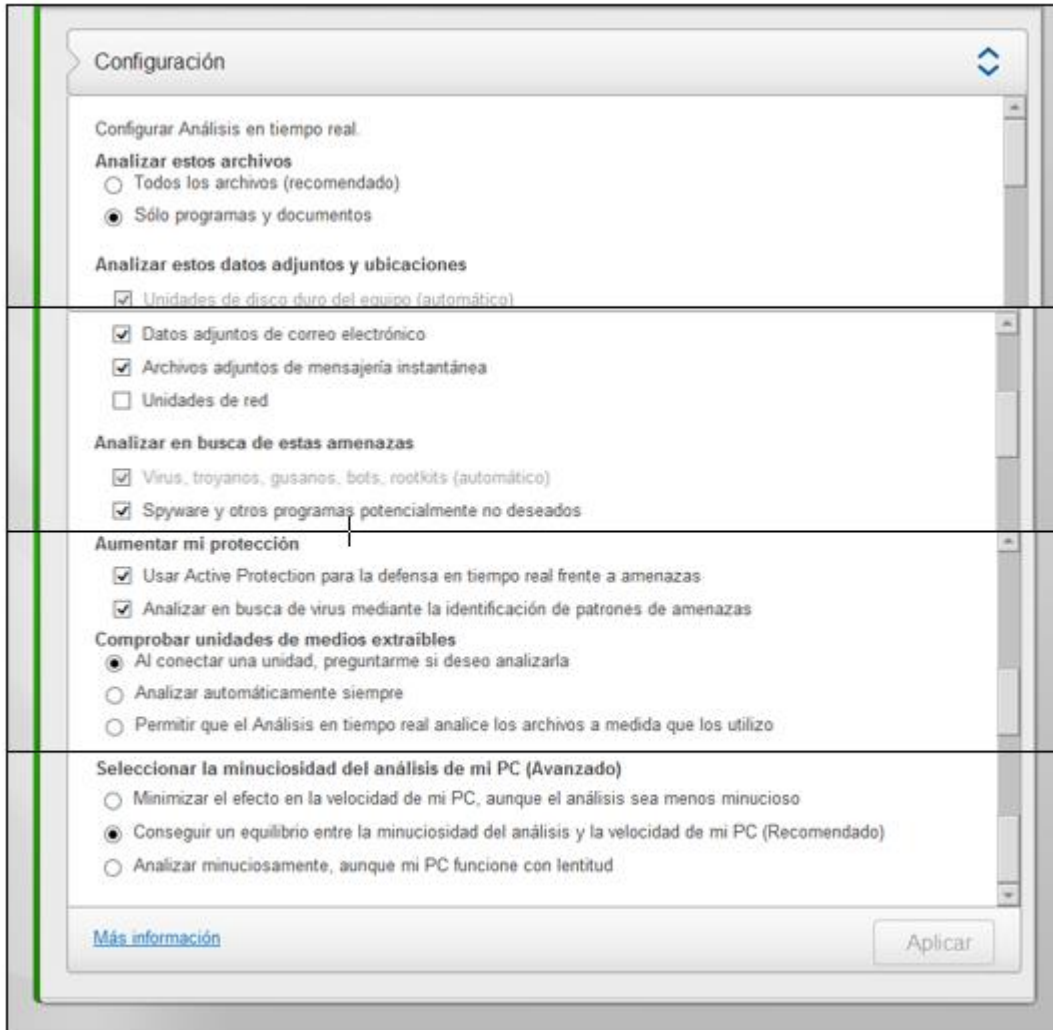


Las opciones de análisis en tiempo real definen lo que McAfee busca durante un análisis en tiempo real, así como la ubicación y los tipos de archivos que analiza. Las opciones incluyen el análisis en busca de virus desconocidos y cookies de rastreo, así como la protección de desbordamiento de búfer.



1.1.1.2.1 Configuración:

Permite elegir los tipos de archivos adjuntos y las ubicaciones que desee analizar y proteger.



Configuración

Configurar Análisis en tiempo real.

Analizar estos archivos

☐ Todos los archivos (recomendado)

☒ Sólo programas y documentos

Analizar estos datos adjuntos y ubicaciones

☒ Unidades de disco duro del equipo (automática)

☒ Datos adjuntos de correo electrónico

☒ Archivos adjuntos de mensajería instantánea

☐ Unidades de red

Analizar en busca de estas amenazas

☒ Virus, troyanos, gusanos, bots, rootkits (automático)

☒ Spyware y otros programas potencialmente no deseados

Aumentar mi protección

☒ Usar Active Protection para la defensa en tiempo real frente a amenazas

☒ Analizar en busca de virus mediante la identificación de patrones de amenazas

Comprobar unidades de medios extraíbles

☒ Al conectar una unidad, preguntarme si deseo analizarla

☐ Analizar automáticamente siempre

☐ Permitir que el Análisis en tiempo real analice los archivos a medida que los utilizo

Seleccionar la minuciosidad del análisis de mi PC (Avanzado)

☐ Minimizar el efecto en la velocidad de mi PC, aunque el análisis sea menos minucioso

☒ Conseguir un equilibrio entre la minuciosidad del análisis y la velocidad de mi PC (Recomendado)

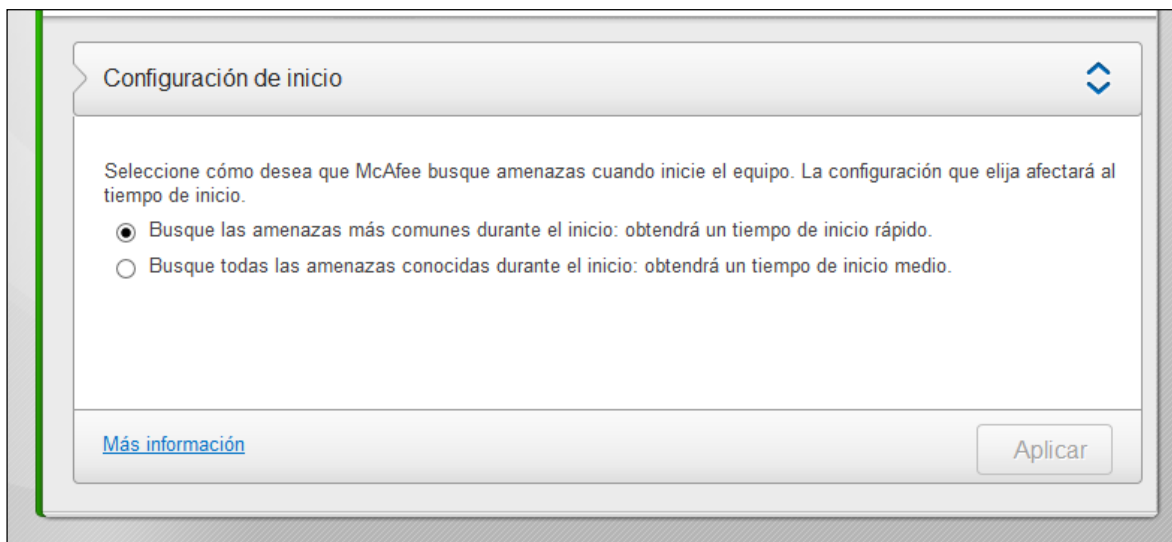
☐ Analizar minuciosamente, aunque mi PC funcione con lentitud

[Más información](#)

Aplicar

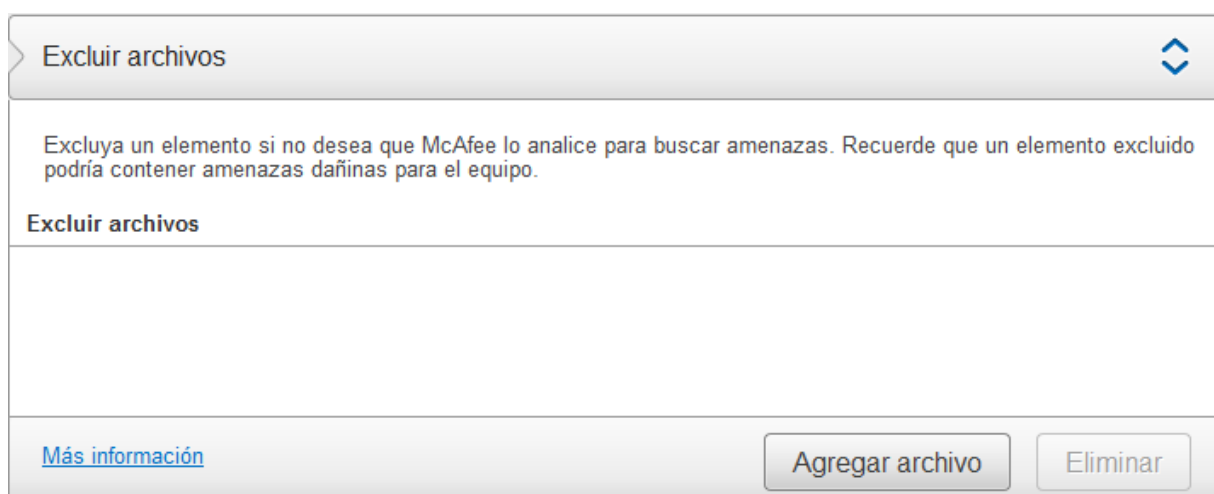
1.1.1.2.2 Configuración de Inicio:

Permite determinar el modo en que desea que McAfee inicie la búsqueda de amenazas.



1.1.1.2.3 Excluir archivos

Permite excluir un elemento si no desea que McAfee lo analice para búsqueda de amenazas.



Tipos de archivos:

Todos los archivo Detectar actividades sospechosas y todos los puntos susceptibles de ataque. El análisis en busca de virus solo se hará en documentos y programas.

Analizar estos archivos	
☐	Todos los archivos (recomendado)
☒	Sólo programas y documentos

Archivos adjuntos y ubicaciones:

- *Datos adjuntos de correo electrónico* Detecta la actividad de virus y otras amenazas en el correo electrónico entrante y saliente.
- *Archivos adjuntos de mensajería instantánea.* Detecta la actividad de virus y otras amenazas en los archivos adjuntos de mensajería instantánea que envía y recibe.
- *Unidades de red.* Detecta la actividad de virus y otras amenazas en las unidades de red, así como en las unidades de disco duro locales.

Analizar estos datos adjuntos y ubicaciones	
☒	Unidades de disco duro del equipo (automático)
☒	Datos adjuntos de correo electrónico
☒	Archivos adjuntos de mensajería instantánea
☐	Unidades de red

Amenazas

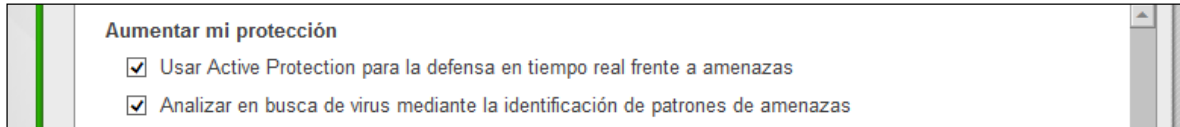
Cookies de rastreo. Detecta cookies de rastreo que controlan sus hábitos de navegación en la Web

- ***Secuencias de comandos en Internet Explorer y Firefox.*** Detecta secuencias de comandos y código malintencionadas que se ejecutan en Internet Explorer y Firefox
- ***Spyware y otros programas potencialmente no deseados.*** Detecta spyware y otros programas potencialmente no deseados
- ***Desbordamientos del búfer.*** Protege el equipo de los desbordamientos del búfer (sobre escritura en la memoria)

Analizar en busca de estas amenazas	
☒	Virus, troyanos, gusanos, bots, rootkits (automático)
☒	Spyware y otros programas potencialmente no deseados

Aumenta mi protección:

- *Active protection proporciona defensa en tiempo real contra los virus, spyware y amenazas recientes directamente en el equipo* Proporciona a su equipo una protección inmediata contra virus y spyware, analizando y bloqueando una nueva amenaza en milisegundos, en lugar de tener que esperar durante horas con las técnicas tradicionales



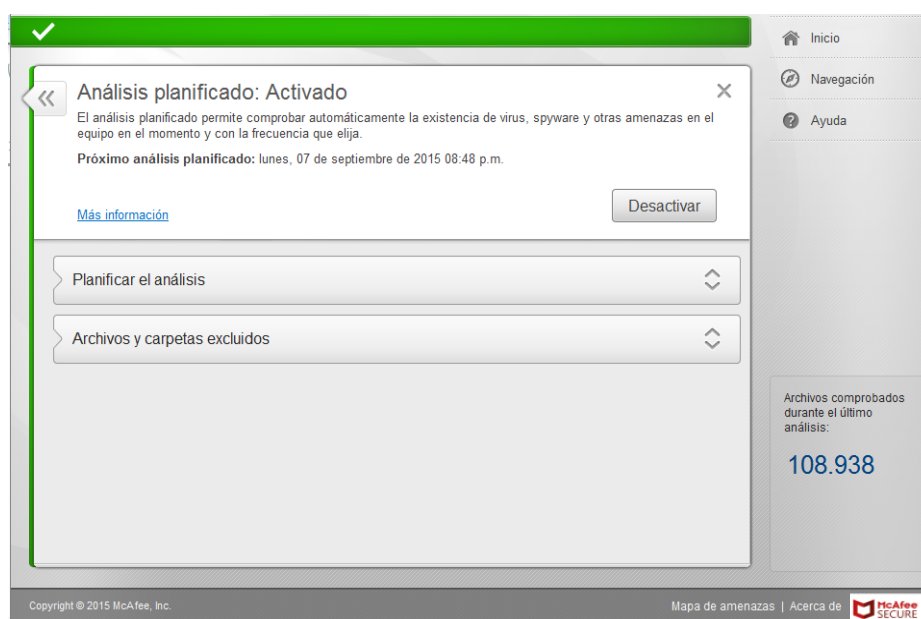
- **Analizar en busca de virus mediante la identificación de patrones de amenazas.** Permite la detección de amenazas que aunque no sean identificadas como tal, presentan comportamientos similares a amenazas ya identificadas. Finalmente para aplicar cualquier cambio realizado, marcamos *Aplicar*.



Tenga cuidado al cambiar las opciones de configuración predeterminadas del análisis en tiempo real, ya que el equipo puede quedar expuesto a ciertas amenazas.

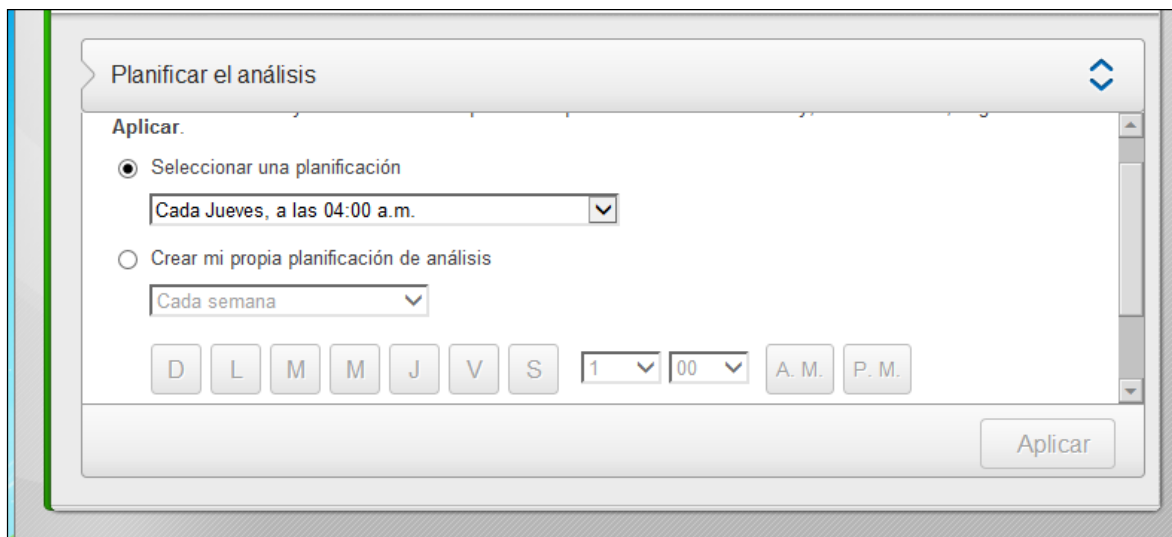
1.1.1.3 Análisis Planificado

Los análisis planificados son uno de los elementos necesarios para asegurar la continua salud del equipo. Comprobado exhaustivamente (*Análisis completo*) el equipo en busca de virus y otras amenazas, de forma automática y periódicamente. Para acceder a la configuración desde el panel de inicio, ingrese a *Protección de antispyware y antivirus*, luego *Análisis planificado*.



1.1.1.3.1 Planificación de análisis personalizado:

Planificación de análisis predeterminada



Planificar el análisis

Aplicar.

☒ Seleccionar una planificación

Cada Jueves, a las 04:00 a.m.

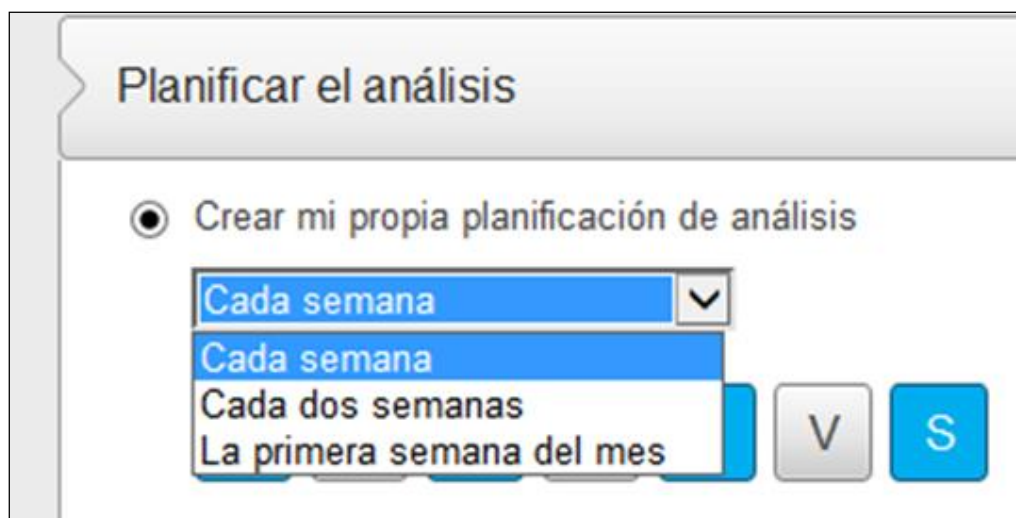
☐ Crear mi propia planificación de análisis

Cada semana

D L M M J V S 1 00 A. M. P. M.

Aplicar

De forma predeterminada, McAfee efectúa un análisis planificado cada martes una vez a la semana a las 4:00, cada dos lunes al mes a las 4:00 o el primer viernes de cada mes a las 4:00.



Planificar el análisis

☒ Crear mi propia planificación de análisis

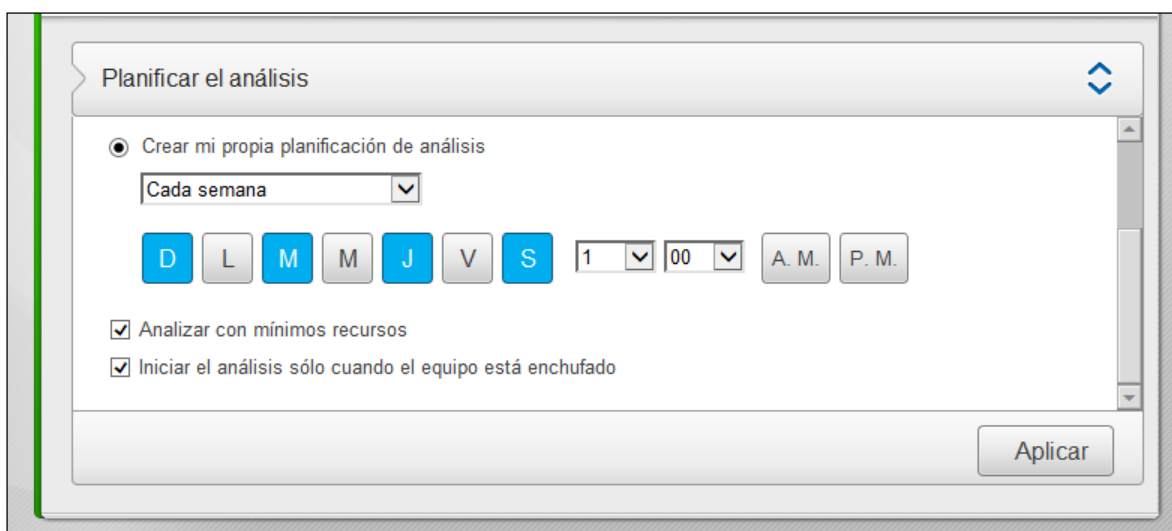
Cada semana

Cada semana

Cada dos semanas

La primera semana del mes

V S



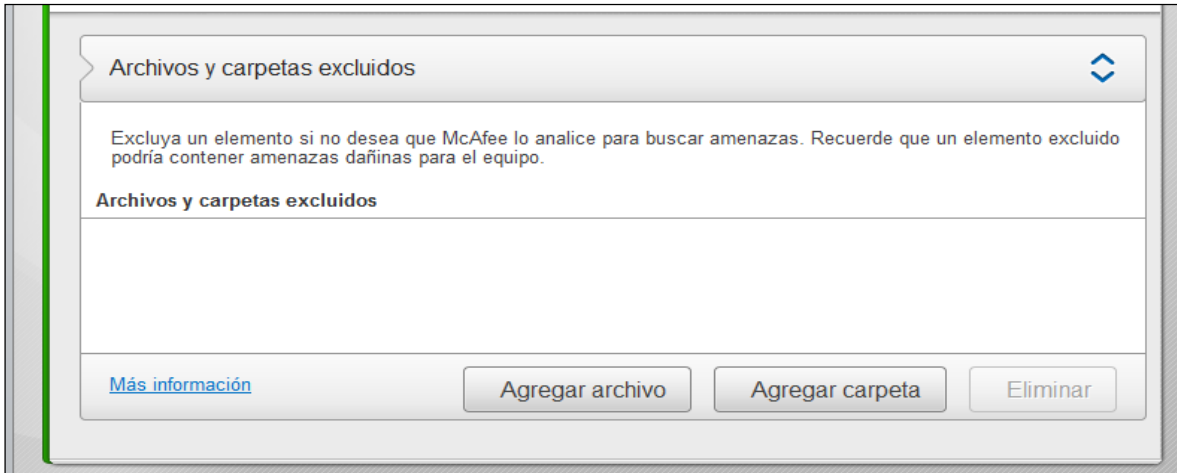
La planificación del análisis también puede modificarse según sus necesidades. Podemos seleccionar si el análisis se hará semanalmente, cada dos semanas o la primera semana de cada mes. Adicionalmente podemos escoger el día o los días y la hora en los cual se realizara el análisis.

Otras opciones

- La opción *Analizar con mínimos recursos* hace que el análisis utilice una mínima de la potencia de procesamiento del computador. Aunque esta opción está activada de forma predeterminada, puede desactivarla para aumentar la velocidad del análisis planificado.
- La opción *Iniciar el análisis solo cuando el equipo está enchufado*, le permite ahorrar batería cuando el Centro de Seguridad de McAfee está en equipos portátiles. El análisis solo se ejecutará hasta que el equipo se encuentre conectado a la toma eléctrica.

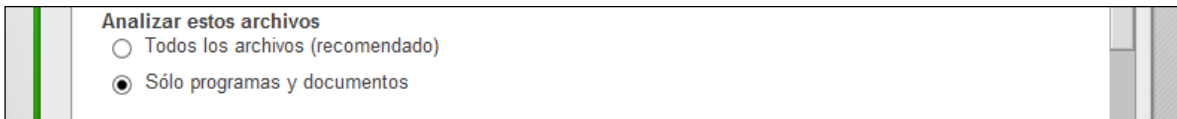
1.1.1.3.2 Archivos y carpetas excluidos

Permite excluir un elemento si no desea que McAfee lo analice para búsqueda de amenazas.



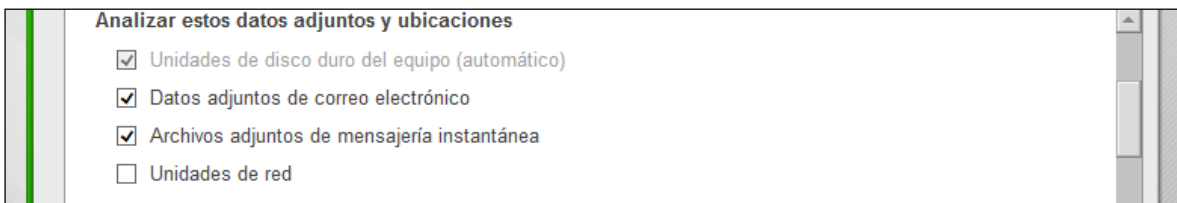
Tipos de archivos:

Todos los archivos Detectar actividades sospechosas y todos los puntos susceptibles de ataque
Solo programas y documentos El análisis en busca de virus solo se hará en documentos y programas.



Archivos adjuntos y ubicaciones:

- *Datos adjuntos de correo electrónico* Detecta la actividad de virus y otras amenazas en el correo electrónico entrante y saliente.
- *Archivos adjuntos de mensajería instantánea.* Detecta la actividad de virus y otras amenazas en los archivos adjuntos de mensajería instantánea que envía y recibe.
- *Unidades de red.* Detecta la actividad de virus y otras amenazas en las unidades de red, así como en las unidades de disco duro locales.



Amenazas

Cookies de rastreo. Detecta cookies de rastreo que controlan sus hábitos de navegación en la Web

- **Secuencias de comandos en Internet Explorer y Firefox.** Detecta secuencias de comandos y código malintencionadas que se ejecutan en Internet Explorer y Firefox
- **Spyware y otros programas potencialmente no deseados.** Detecta spyware y otros programas potencialmente no deseados
- **Desbordamientos del búfer.** Protege el equipo de los desbordamientos del búfer (sobre escritura en la memoria)

Analizar en busca de estas amenazas	
☒	Virus, troyanos, gusanos, bots, rootkits (automático)
☒	Spyware y otros programas potencialmente no deseados

Aumenta mi protección:

- **Active protection proporciona defensa en tiempo real contra los virus, spyware y amenazas recientes directamente en el equipo** Proporciona a su equipo una protección inmediata contra virus y spyware, analizando y bloqueando una nueva amenaza en milisegundos, en lugar de tener que esperar durante horas con las técnicas tradicionales

Aumentar mi protección	
☒	Usar Active Protection para la defensa en tiempo real frente a amenazas
☒	Analizar en busca de virus mediante la identificación de patrones de amenazas

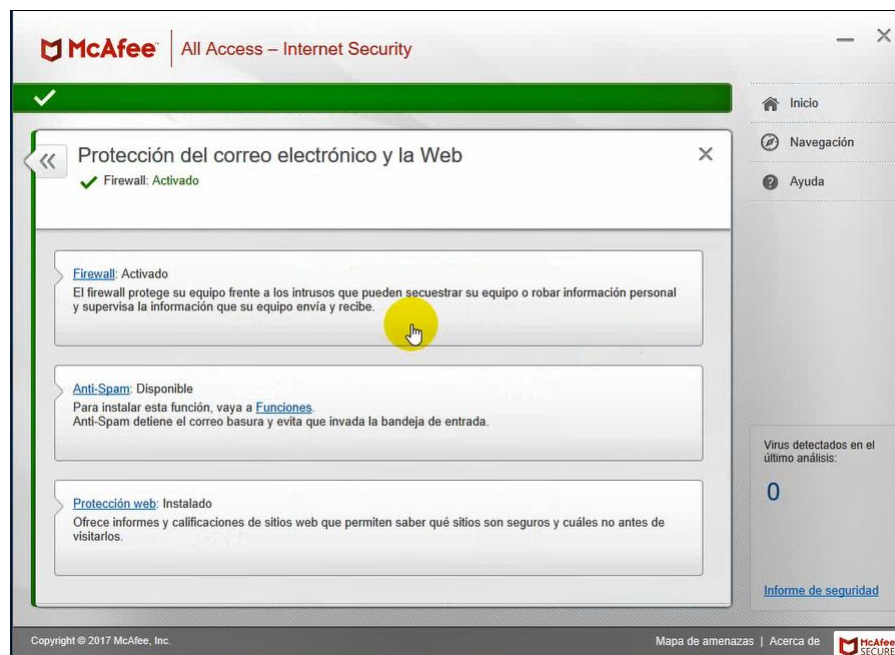
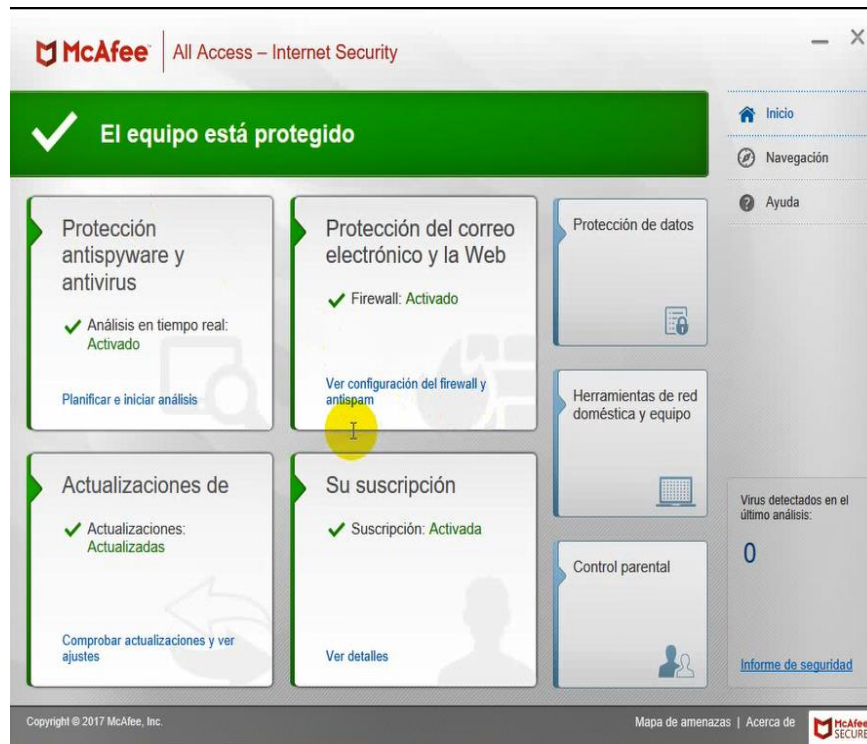
- **Analizar en busca de virus mediante la identificación de patrones de amenazas.** Permite la detección de amenazas que aunque no sean identificadas como tal, presentan comportamientos similares a amenazas ya identificadas. Finalmente para aplicar cualquier cambio realizado, marcamos *Aplicar*.



Tenga cuidado al cambiar las opciones de configuración predeterminadas del análisis en tiempo real, ya que el equipo puede quedar expuesto a ciertas amenazas.

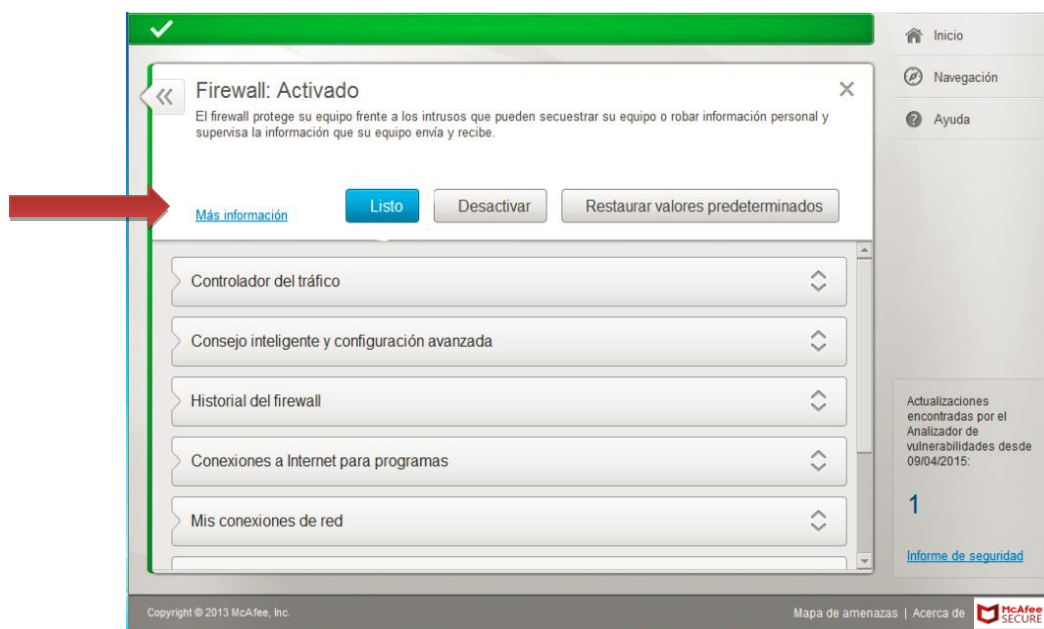
1.1.2 Protección del Correo Electrónico y la web:

El Firewall de McAfee actúa como una barrera defensiva entre Internet y el equipo, lo que le permite controlar tanto lo que entra como lo que sale. La funcionalidad de Firewall se ha diseñado especialmente para supervisar el tráfico de Internet en busca de actividades sospechosas y para proporcionar una protección eficaz sin interrumpirle en sus actividades.



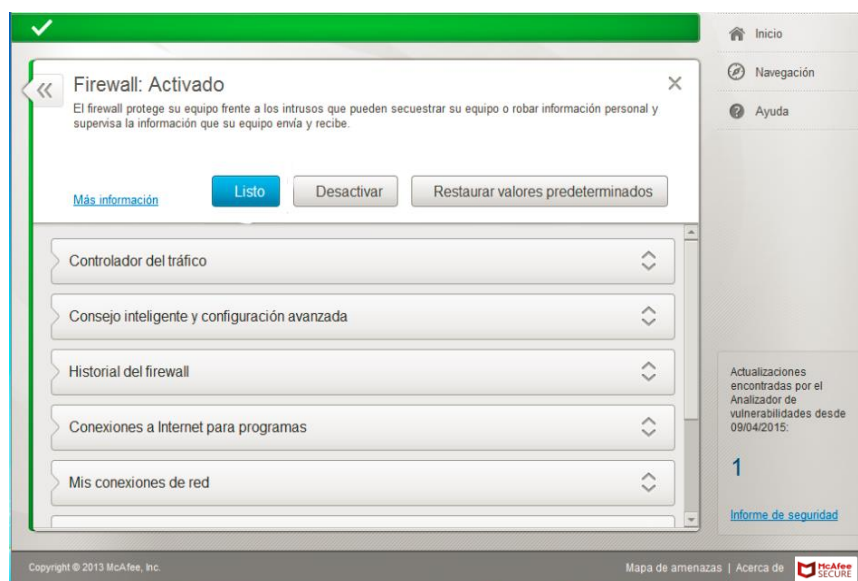
1.1.2.1 Firewall:

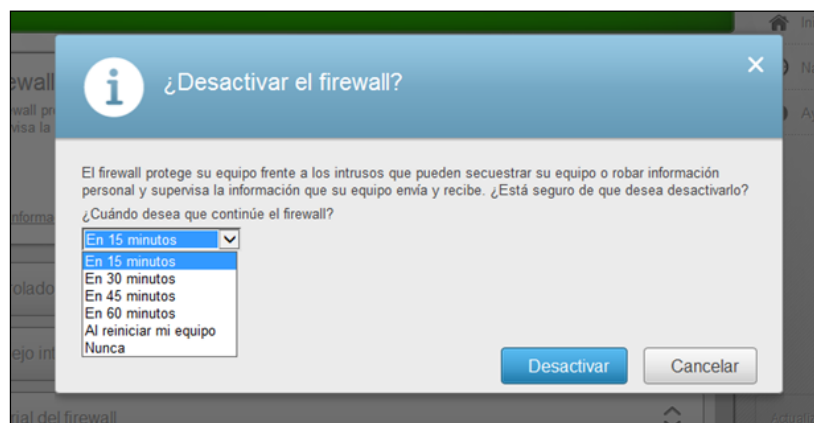
Desde el momento en el que instala el Firewall, éste empieza a proteger el equipo frente a intrusiones y tráfico de red no deseado. De forma predeterminada, el Firewall está configurado para autorizar el acceso saliente a los programas.



1.1.2.1.1 Desactivar

Puede desactivar el Firewall si lo necesita (por ejemplo, para la solución de problemas o realización de pruebas), pero si lo hace, el equipo dejará de estar protegido frente a las intrusiones y el tráfico de red no deseado. Tampoco podrá administrar las conexiones a Internet entrantes y salientes. Si desactiva la protección por firewall vuelva a activarlo lo antes posible.





En la ventana de confirmación decida cuándo se reiniciara el firewall haciendo clic en la flecha situada junto a la opción *¿Cuándo desea que continúe el firewall?* El valor predeterminado es 15 minutos. Por último haga clic en *Desactivar*.

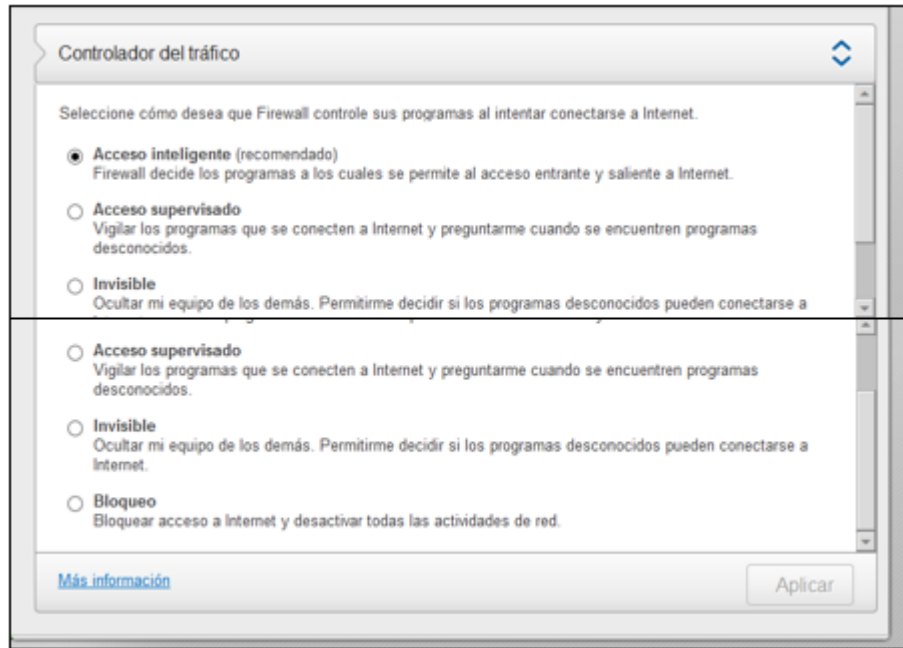


La desactivación de **Firewall** deja al equipo expuesto a las amenazas y el estado de la protección de la **Página de inicio** cambia e indica que el equipo está "en riesgo".

Para reactivar nuevamente el Firewall, ingresamos desde el panel de inicio a *Firewall* (1) y luego *Configuración* (2). Luego *Activar*



1.1.2.1.2 Controlador de Tráfico:



Controlador del tráfico

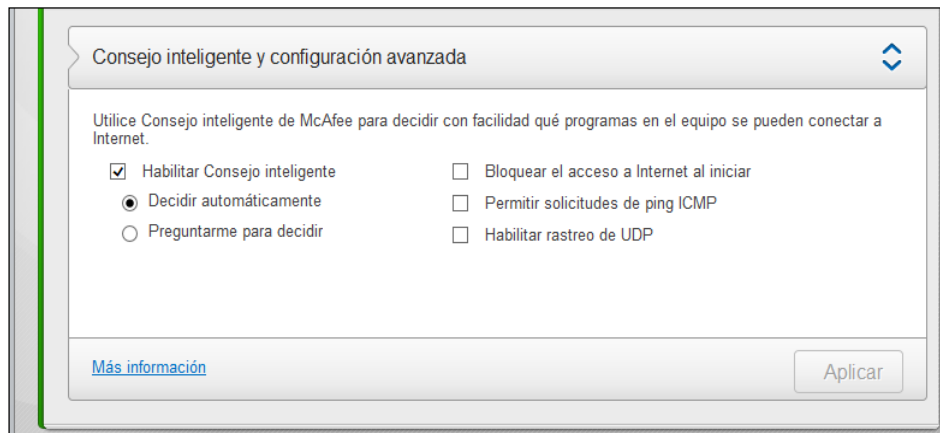
Seleccione cómo desea que Firewall controle sus programas al intentar conectarse a Internet.

- ☒ **Acceso inteligente (recomendado)**
Firewall decide los programas a los cuales se permite el acceso entrante y saliente a Internet.
- ☐ **Acceso supervisado**
Vigilar los programas que se conecten a Internet y preguntarme cuando se encuentren programas desconocidos.
- ☐ **Invisible**
Ocultar mi equipo de los demás. Permitirme decidir si los programas desconocidos pueden conectarse a Internet.

- ☐ **Acceso supervisado**
Vigilar los programas que se conecten a Internet y preguntarme cuando se encuentren programas desconocidos.
- ☐ **Invisible**
Ocultar mi equipo de los demás. Permitirme decidir si los programas desconocidos pueden conectarse a Internet.
- ☐ **Bloqueo**
Bloquear acceso a Internet y desactivar todas las actividades de red.

[Más información](#) Aplicar

1.1.2.1.3 Consejo inteligente y configuración avanzada



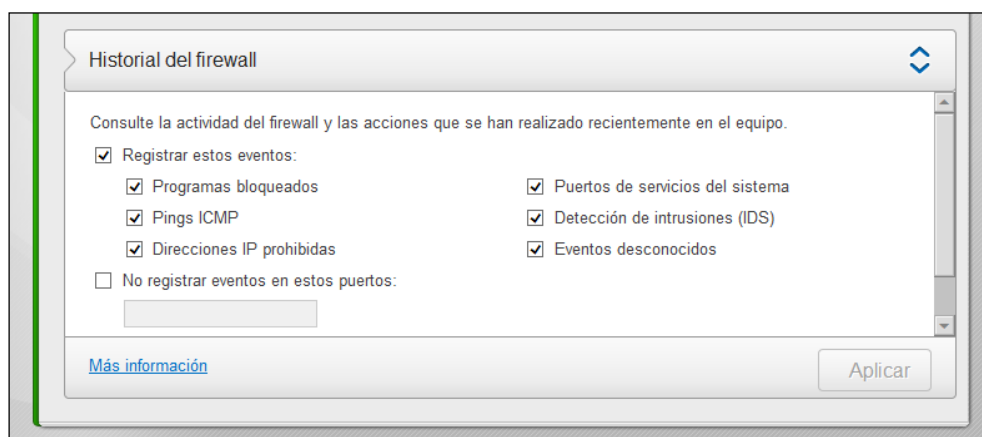
Consejo inteligente y configuración avanzada

Utilice Consejo inteligente de McAfee para decidir con facilidad qué programas en el equipo se pueden conectar a Internet.

☒ Habilitar Consejo inteligente	☐ Bloquear el acceso a Internet al iniciar
☒ Decidir automáticamente	☐ Permitir solicitudes de ping ICMP
☐ Preguntarme para decidir	☐ Habilitar rastreo de UDP

[Más información](#) Aplicar

1.1.2.1.4 Historial de Firewall



Historial del firewall

Consulte la actividad del firewall y las acciones que se han realizado recientemente en el equipo.

☒ Registrar estos eventos:

☒ Programas bloqueados	☒ Puertos de servicios del sistema
☒ Pings ICMP	☒ Detección de intrusiones (IDS)
☒ Direcciones IP prohibidas	☒ Eventos desconocidos

☐ No registrar eventos en estos puertos:

[Más información](#) Aplicar

1.1.2.1.5 Conexiones a Internet para programas

Conexiones a Internet para programas		
Decida qué programas pueden acceder a Internet y utilice Net Guard para evitar que realicen conexiones peligrosas.		
Programa	Acceso	Net Guard
> Aplicación de servicios y controlador	Completo	Activado
> Proceso host para los servicios de Windows	Completo	Activado
> Google Chrome	Completo	Activado
> McAfee Service Host	Completo	Activado
> McAfee Hacker/Watch Update Helper	Completo	Desactivado
> McAfee UI Host	Completo	Desactivado
> McAfee Update Launcher	Completo	Desactivado
> Asistencia remota de Windows	Completo	Activado
> Servidor COM de asistencia remota de Windows	Completo	Activado
> Internet Explorer	Completo	Activado
> SiteAdvisor	Completo	Desactivado
Más información Editar Agregar Eliminar		

1.1.2.1.6 Mis Conexiones de Red

Mis conexiones de red

El firewall le ayuda a seleccionar el mejor equilibrio de seguridad para su equipo dondequiera que esté (en casa, en el trabajo o en un lugar público, como un hotspot Wi-Fi). Puede decidir la red en la que confía y durante cuánto tiempo. Si cambia el tipo de red aquí, debe actualizar también el tipo de red en el Centro de redes y recursos compartidos de Windows.

Red	Tipo de red	Tipo de adaptador
192.168.173.0 - 192.168.173.255	Doméstico	Con cable

[Más información](#)

Editar

Agregar

Eliminar

1.1.2.1.7 Puertos y Servicios del sistema

Puertos y servicios del sistema

Abra un puerto de su equipo para que otros equipos de la red y de Internet puedan acceder a un servicio.

Nombre	Puertos	Descripción
☐ Puerto del servidor de directorio de Microsoft (MSFT DS) 445	Puertos TCP/IP locales:445	Puerto del servidor de directorio

[Más información](#)

Editar

Agregar

Eliminar

1.1.2.1.8 Detección de Intrusiones:

Detección de intrusiones

Protéjase frente a piratas informáticos que traten de aprovechar vulnerabilidades en su sistema operativo o en sus programas para tomar el control de su equipo.

☐ Usar protección frente a intrusiones

- ☒ Básica: Detecta actividades que tengan una alta probabilidad de ser ataques. (Recomendado)
- ☐ Alta: Detecta actividades sospechosas, aunque algunas podrían no ser ataques.

[Más información](#)

Aplicar

1.1.2.1.9 Net Guard:

Net Guard

Net Guard le ayuda a evitar conexiones peligrosas y le permite decidir cuáles desea permitir.

☒ Activar Net Guard (Recomendado)

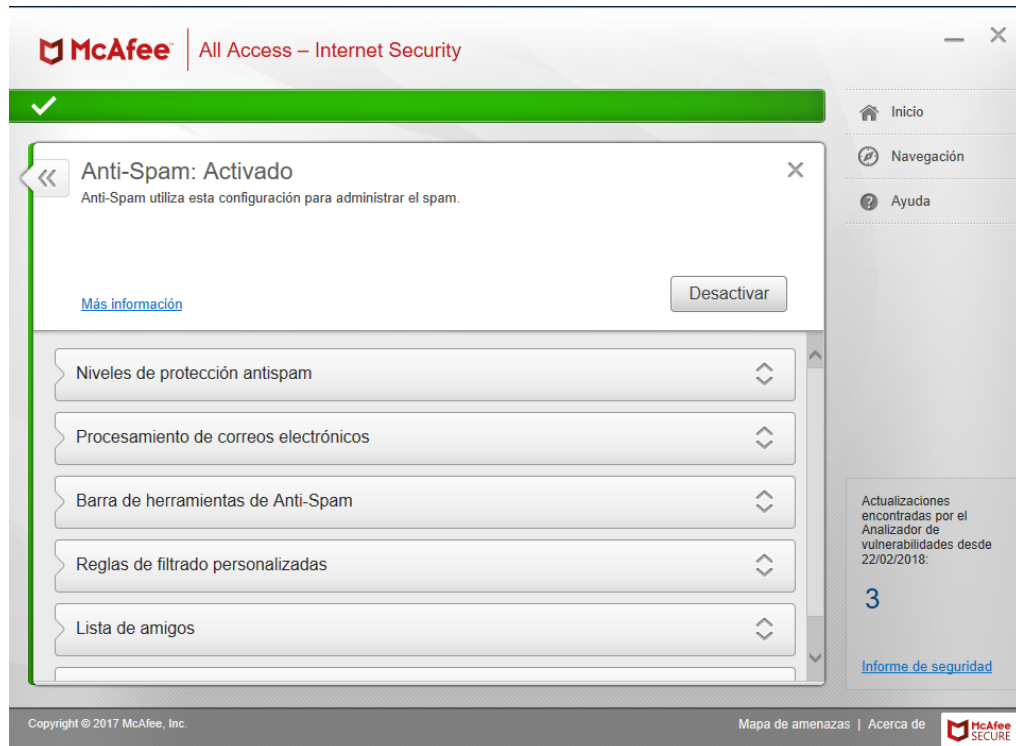
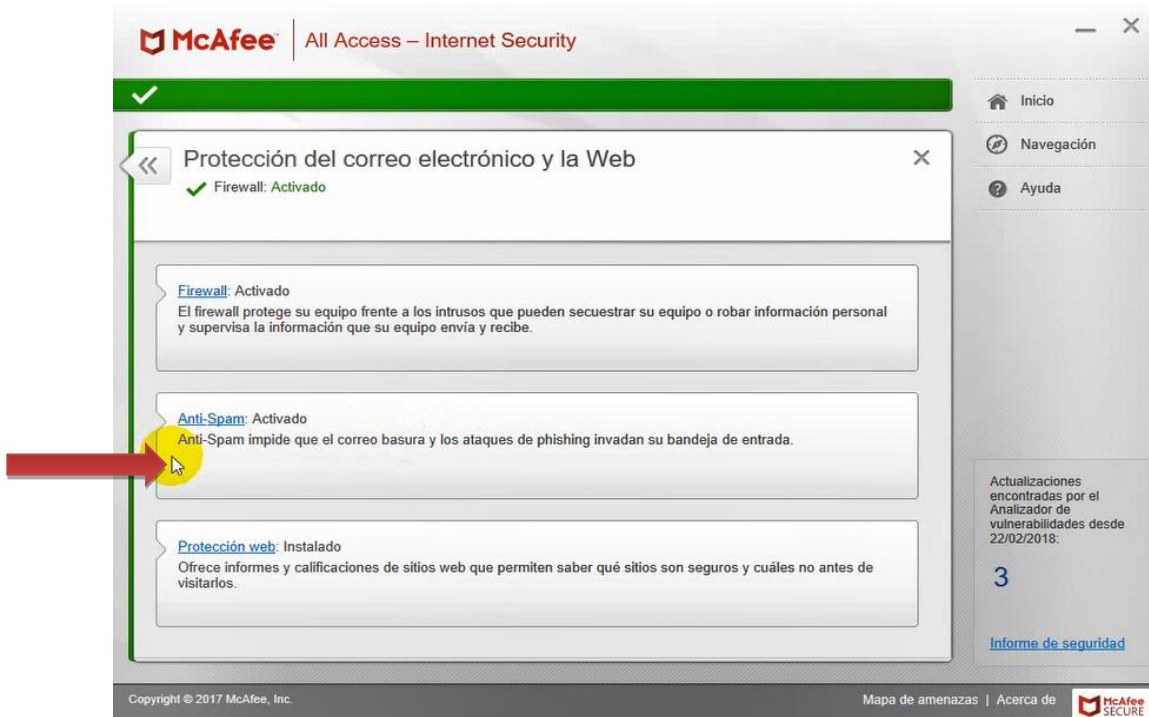
Dirección IP	Último intento de conexión	Acción

[Más información](#)

Editar

Eliminar

1.1.2.2 Anti-Spam:



1.1.2.2.1 Niveles de protección Anti-Spam

Niveles de protección antisпам

Decida cómo Anti-Spam filtra el correo electrónico para proteger la bandeja de entrada local del spam.

- ☐ Mínimo
Llegará más spam a la bandeja de entrada.
- ☐ Limitado
Sólo llegará algo de spam a la bandeja de entrada.
- ☒ Equilibrado (recomendado)
Minimiza el número de mensajes de correo electrónico identificados como spam o no spam de forma incorrecta.
- ☐ Agresivo
Apenas llegará spam a la bandeja de entrada pero muchos mensajes de correo electrónico se identificarán

[Más información](#) Aplicar

1.1.2.2.2 Procesamiento de correos electrónicos

Procesamiento de correos electrónicos

Anti-Spam utiliza esta configuración para administrar el spam.

Después de marcar el correo electrónico como phishing o spam:

- ☒ Mover el correo electrónico a la carpeta de Anti-Spam
- ☐ Dejar el correo electrónico en el buzón de entrada

Etiquetar el correo electrónico de spam o phishing como:

[SPAM] para spam
[PHISH] para phishing

[Más información](#) Aplicar

1.1.2.2.3 Barra de herramientas Anti-Spam

Barra de herramientas de Anti-Spam

Vea la barra de herramientas de Anti-Spam en estos programas.

☒ Outlook ☒ Thunderbird

[Más información](#) Aplicar

1.1.2.2.4 Reglas de filtrado personalizadas

Reglas de filtrado personalizadas

Proporcione protección personalizada para la bandeja de entrada mediante el ajuste del modo en que Anti-Spam filtra el correo electrónico.

Campo	Condición	Palabra o frase	Acción

[Más información](#)
Editar
Agregar
Eliminar

1.1.2.2.5 Lista de amigos

Lista de amigos

Permita siempre el correo electrónico de estas direcciones y dominios.

Nombre	Dirección de correo electrónico	Tipo

[Más información](#)
Editar
Agregar
Importar
Eliminar

1.1.2.2.6 Conjunto de caracteres

Conjuntos de caracteres

Un conjunto de caracteres está compuesto por letras y otros símbolos utilizados para visualizar un idioma. Decida si Anti-Spam bloqueará o permitirá entrar correo electrónico en función de su conjunto de caracteres.

Idioma	Código de caracteres	Acción
Árabe	WINDOWS-1256;ISO-8859-6;IBM864;X-MAC-ARABIC	Permitir
Báltico	WINDOWS-1257;ISO-8859-4;ISO-8859-13	Permitir

[Más información](#)
Editar



1.1.2.2.7 Reglas de filtrado de Webmail

Reglas de filtrado de webmail

Proteja la bandeja de entrada local frente a spam filtrando mensajes de webmail.

Dirección de webmail	Tipo de cuenta
----------------------	----------------

[Más información](#)

Editar

Agregar

Eliminar

1.1.2.2.8 Webmail filtrado

Webmail filtrado

Estos mensajes de webmail se han filtrado en busca de spam.

Fecha	De	Asunto
-------	----	--------

[Más información](#)

Vista previa

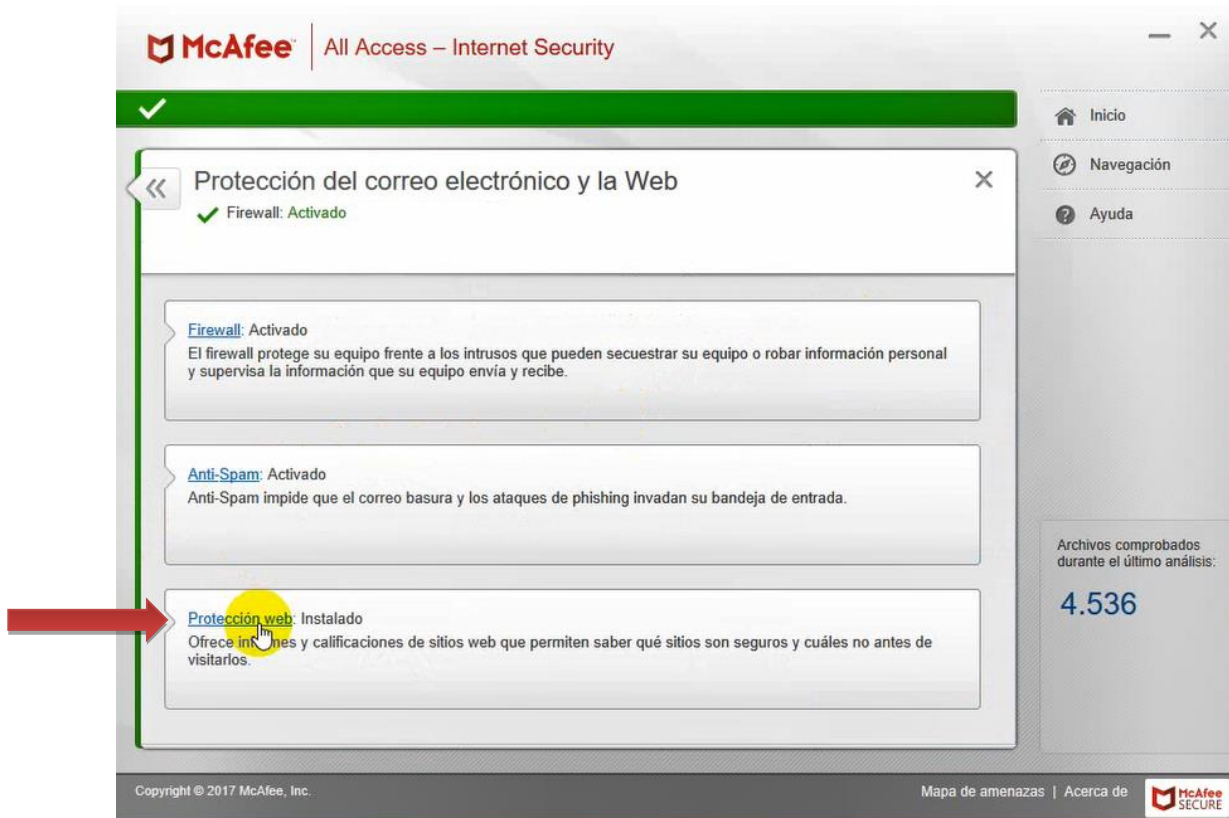
Ver

Exportar

Eliminar

1.1.2.3 SiteAdvisor:

El software Site Advisor es una innovadora herramienta fácil de usar que ayuda a mantener a los usuarios alejados de sitios Web riesgosos y los guía a sitios seguros. Cuenta con dos partes principales: un explorador de la Web que prueba cualquier sitio, el cual se encuentran en busca de amenazas que pueden dañar su equipo y un plug-in (ventana emergente) de explorador que muestra a los usuarios los resultados de nuestras pruebas para los sitios que desean visitar.



¿Cómo califica los sitios Site Advisor?

McAfee usa técnicas propias de recolección y análisis de datos para visitar sitios y reunir información acerca del comportamiento de un sitio Web. SiteAdvisor usa anotaciones tipo semáforo de comprensión universal para calificar los sitios en: rojo, amarillo, verde o gris según su nivel de amenaza.

- Verde = Sitio con Acceso Libre.
- Amarillo = Sitio que merece una mayor atención.
- Rojo = Sitio infectado por virus.
- Gris = El sitio todavía no ha sido verificado y por eso, no hay status.



[Soporte](#)
[Acerca de McAfee](#)
[Póngase en contacto con nosotros](#)
[España - Español](#)

[Inicio](#)
[Seguridad Web](#)
[¿Cómo funciona?](#)
[Descargar](#)
[Recursos](#)
[Administradores del sitio Web](#)

[Inicio](#) / [¿Cómo funciona?](#)



¿Qué es el software SiteAdvisor?

El software SiteAdvisor es un galardonado complemento gratuito para navegadores que ofrece asesoramiento sobre distintos aspectos de la seguridad de los sitios Web *antes* de hacer clic en éstos.

¿Cómo funciona?

Con el software SiteAdvisor instalado, el navegador adoptará un aspecto ligeramente distinto. Se incorporarán pequeños iconos de clasificaciones de los sitios a los resultados de búsqueda, así como un botón de navegador y un cuadro de búsqueda opcional. Conjuntamente, estos elementos le alertarán de los posibles riesgos asociados a los sitios, y le ayudarán a encontrar alternativas más seguras.

Estas clasificaciones de sitios se basan en pruebas que McAfee efectúa armado con todo un ejército de equipos que buscan amenazas de todo tipo (a continuación, encontrará más detalles al respecto). El resultado es una auténtica guía de navegación segura en Web.

La tecnología SiteAdvisor es gratuita; su instalación, fácil de usar; y su uso, aún más sencillo. Además,

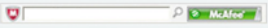
Descargar el software SiteAdvisor

El software SiteAdvisor funciona con Internet Explorer (sólo Windows) y Firefox (Mac y Windows). McAfee clasifica más del 95% de la Web para su seguridad.

[Descarga gratuita](#)

Novedad. Cuadro de Secure Search

Ahora, podrá incorporar un cuadro de Secure Search al navegador para que buscar en la Web de un modo seguro sea más fácil que nunca.



Use el cuadro para bloquear los sitios peligrosos, evitar errores ortográficos y satisfacer todas las

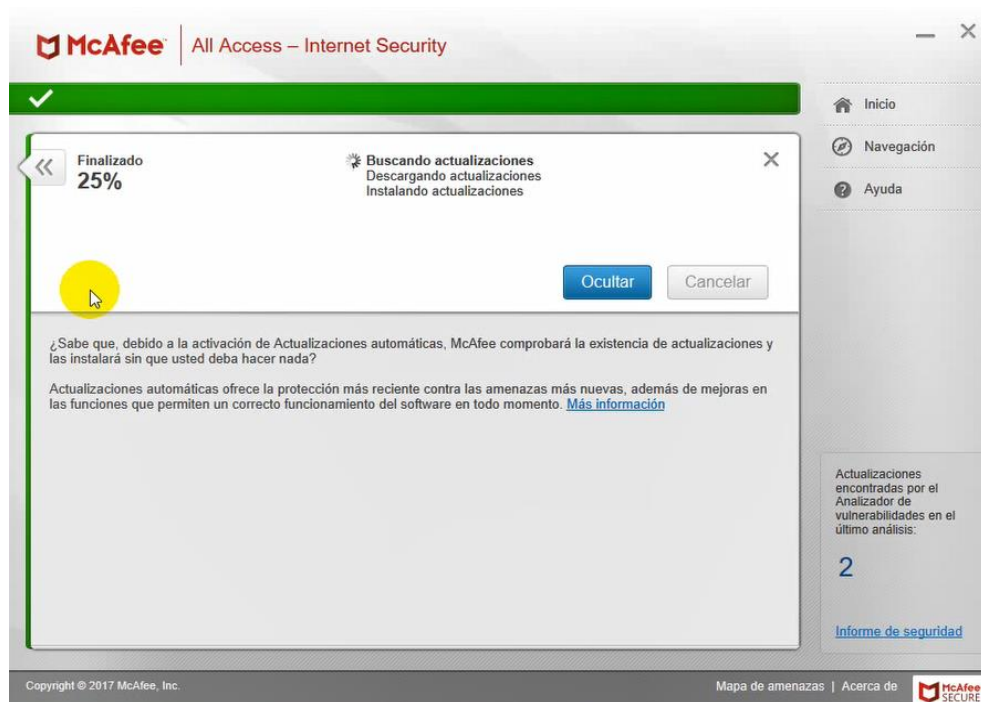
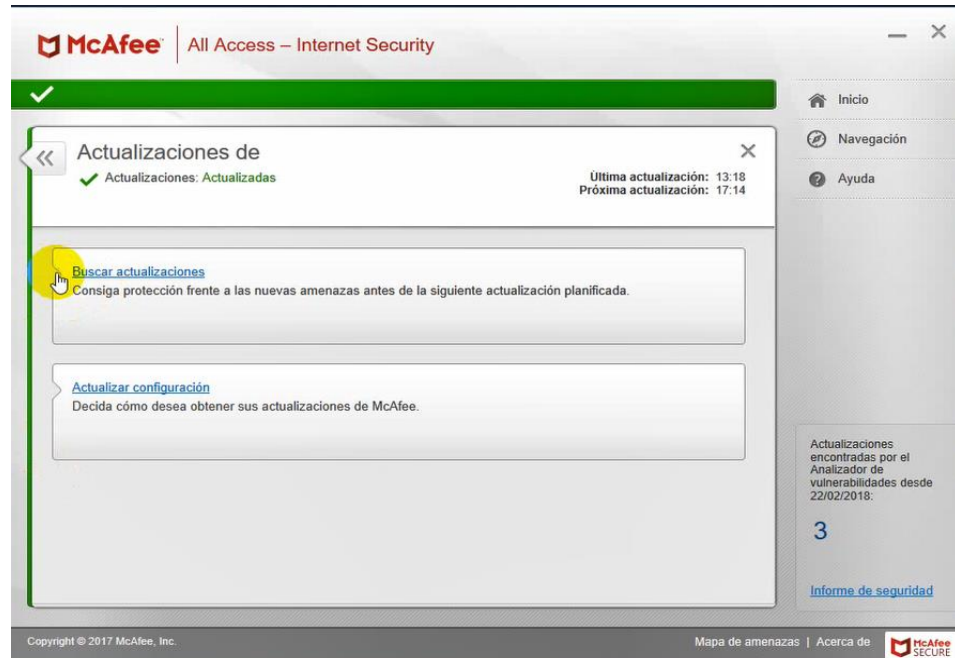
1.1.3 Actualizaciones de McAfee

Permanezca protegido frente amenazas y consiga actualizaciones de funciones que permiten que el software funcione correctamente.



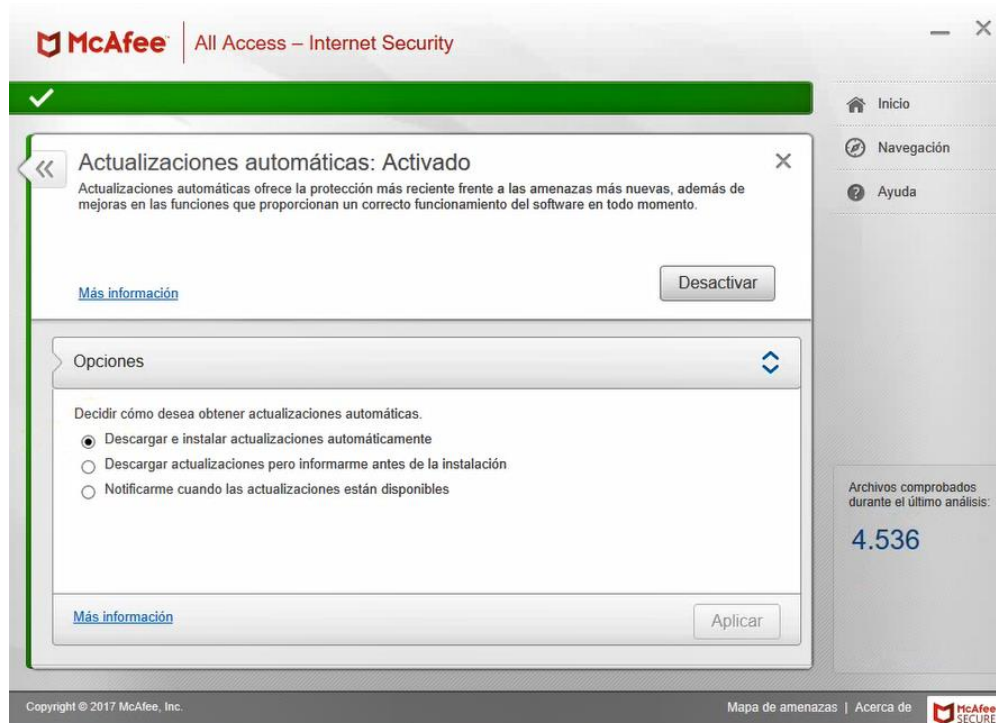
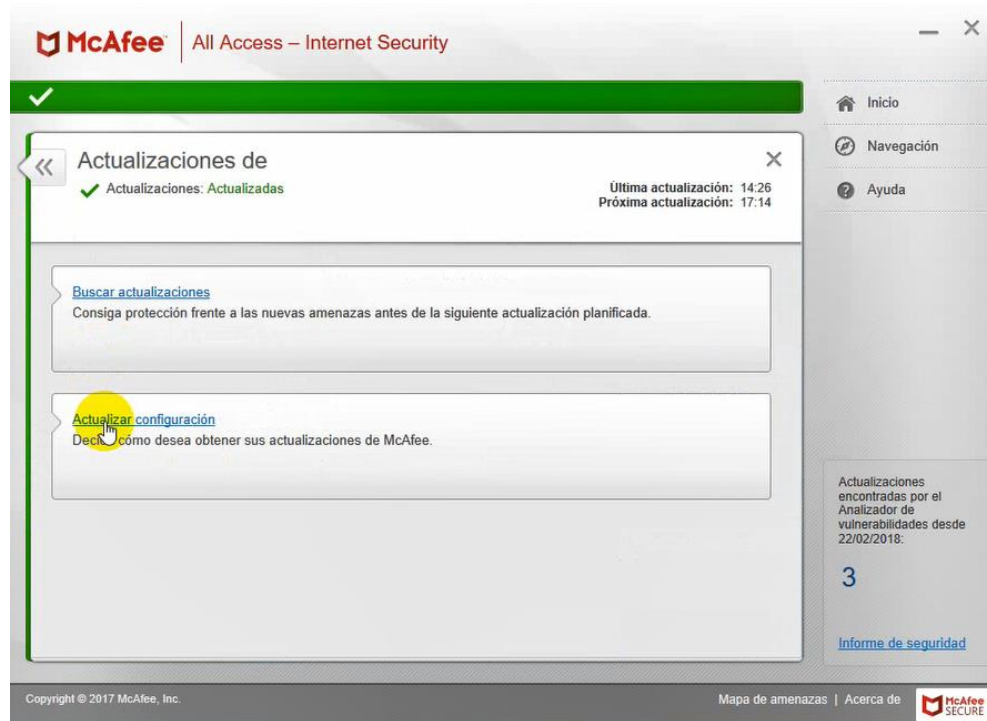
1.1.3.1 Buscar actualizaciones

Consiga protección frente a nuevas amenazas antes de la siguiente actualización planificada.



1.1.3.2 Actualizar configuración

Decida cómo desea obtener sus actualizaciones de McAfee

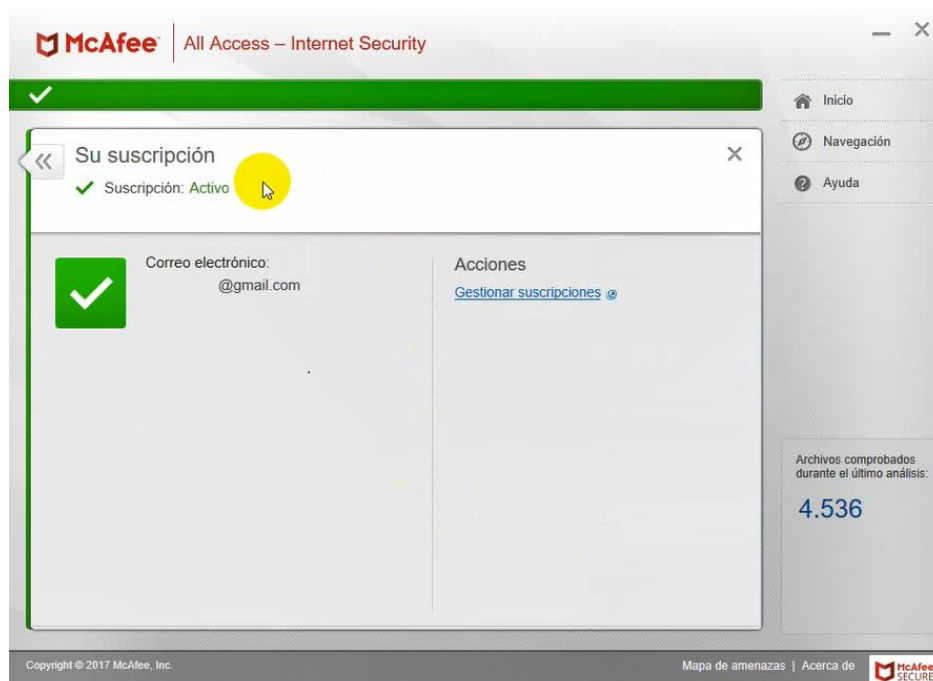


1.1.4 Su suscripción

Cada producto de protección McAfee que adquiera incluye una suscripción que le permite utilizar el producto en un determinado número de equipos durante un período de tiempo.

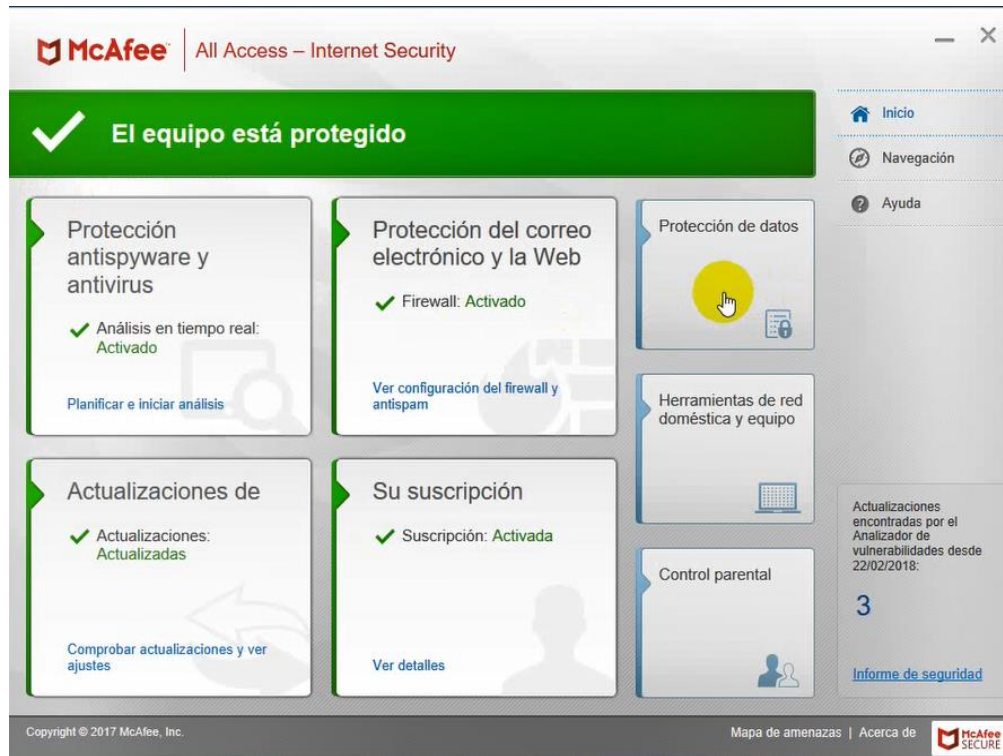


La duración de la suscripción varía en función de su adquisición, pero normalmente comienza al activar el producto.



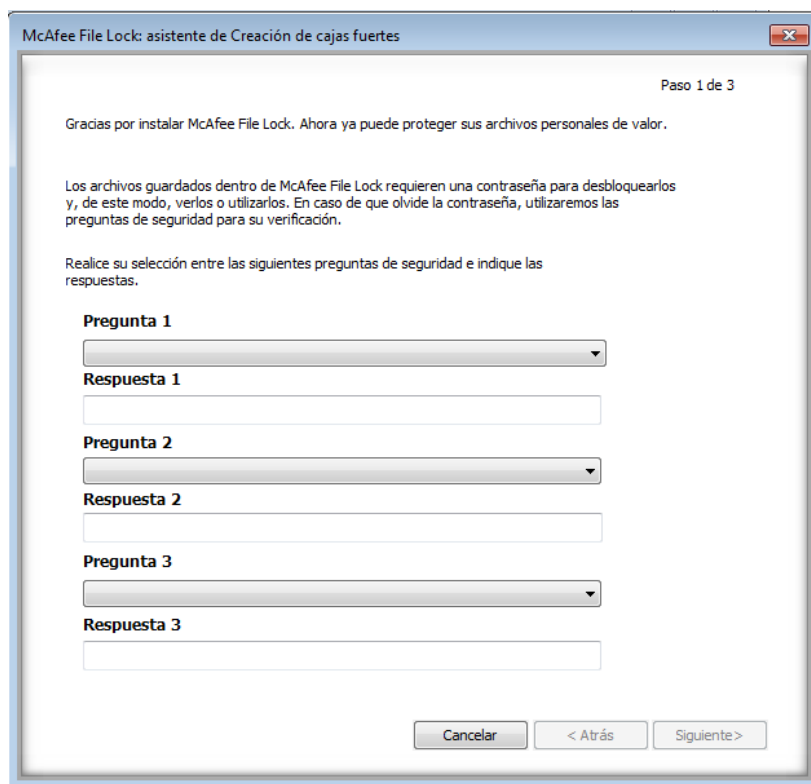
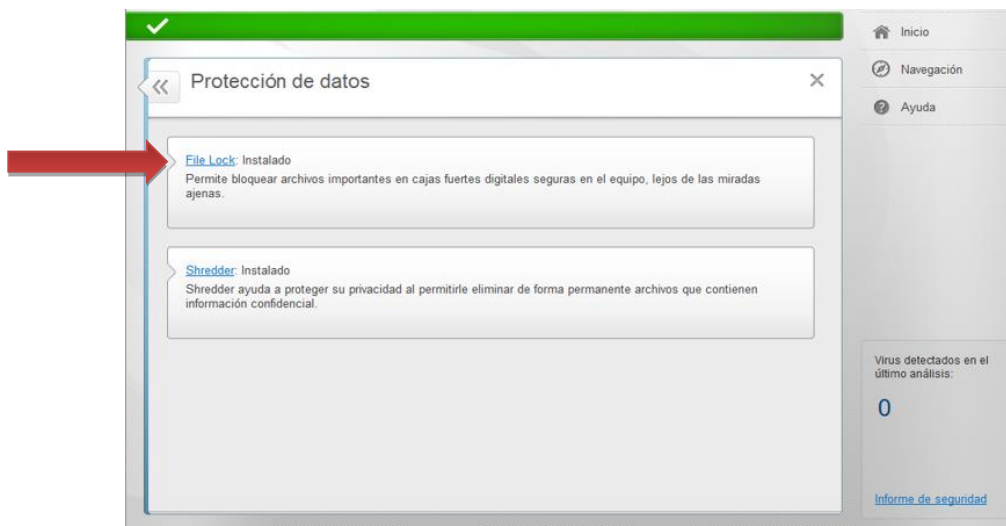
1.1.5 Protección de datos

La protección de McAfee de datos se hace a través de su herramienta Shredder. Esta protege la privacidad eliminando de forma permanente archivos que contienen información confidencial.



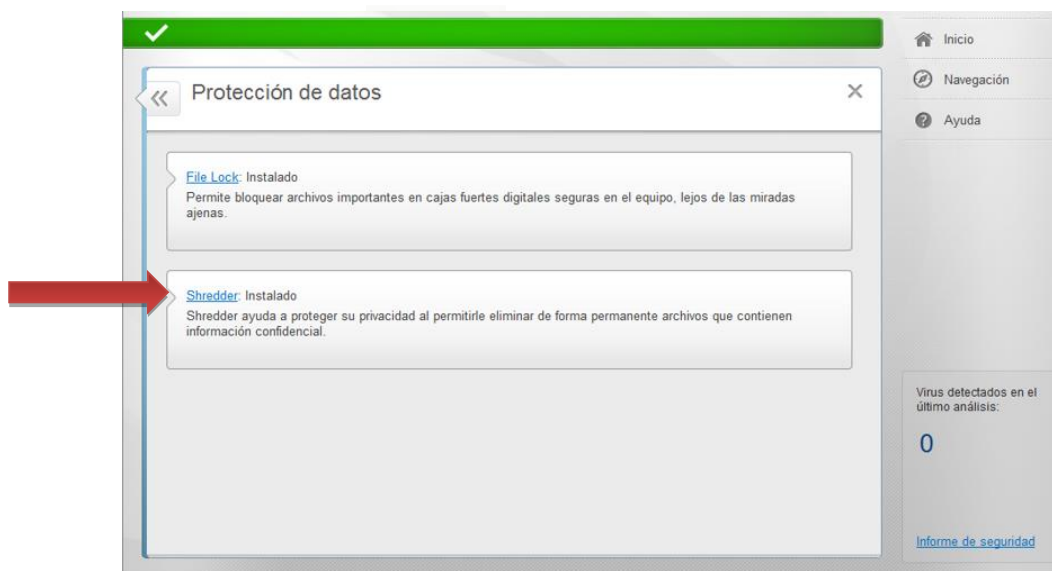
1.1.5.1 FileLock

Permite bloquear archivos importantes en cajas fuertes digitales seguras en el equipo, lejos de las miradas ajenas.

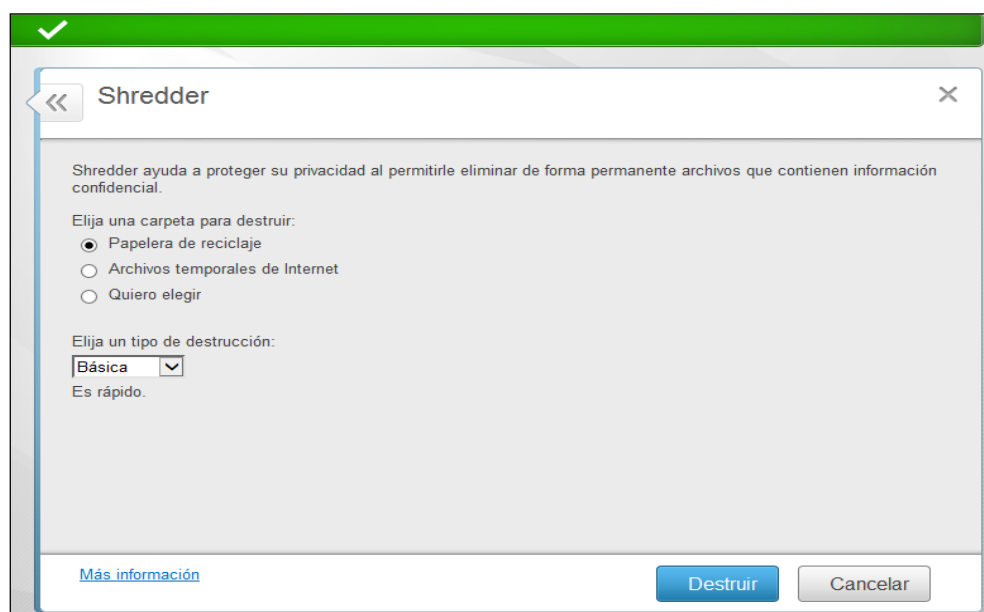


1.1.5.2 Shredder:

Shredder le ayudará a proteger su privacidad al permitirle eliminar de forma permanente archivos que contienen información confidencial.



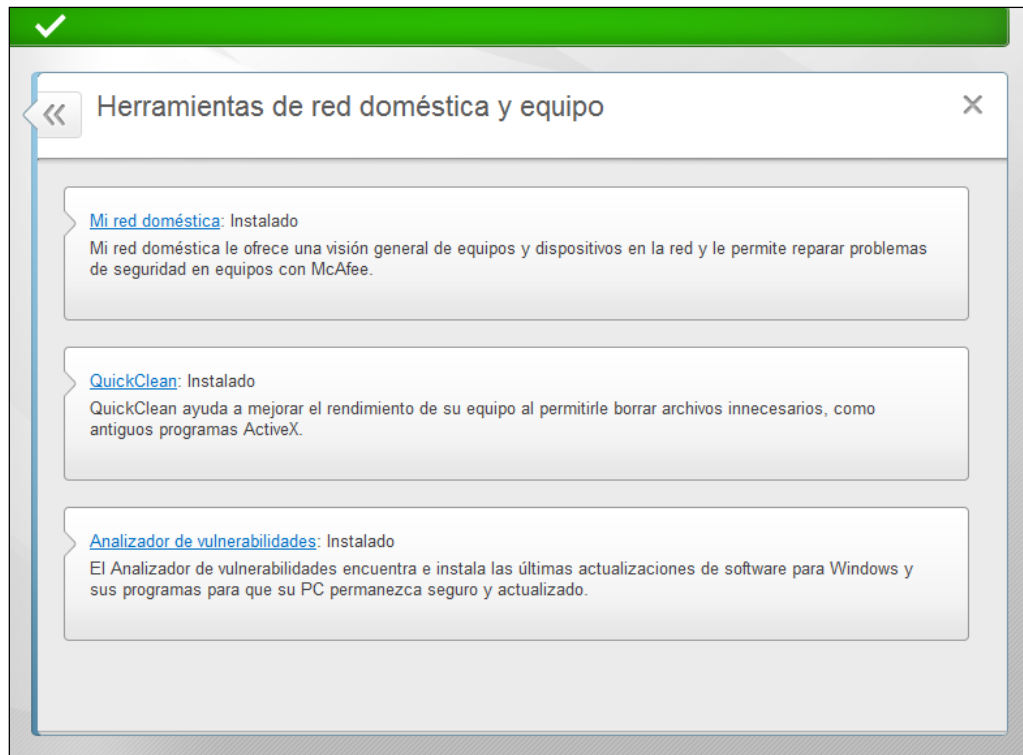
Puede elegir destruir los archivos de la Papelera de reciclaje, Archivos temporales, además de poder realizar una destrucción rápida, básica, segura, exhaustiva o completa.



1.1.6 Herramientas de red doméstica y equipo

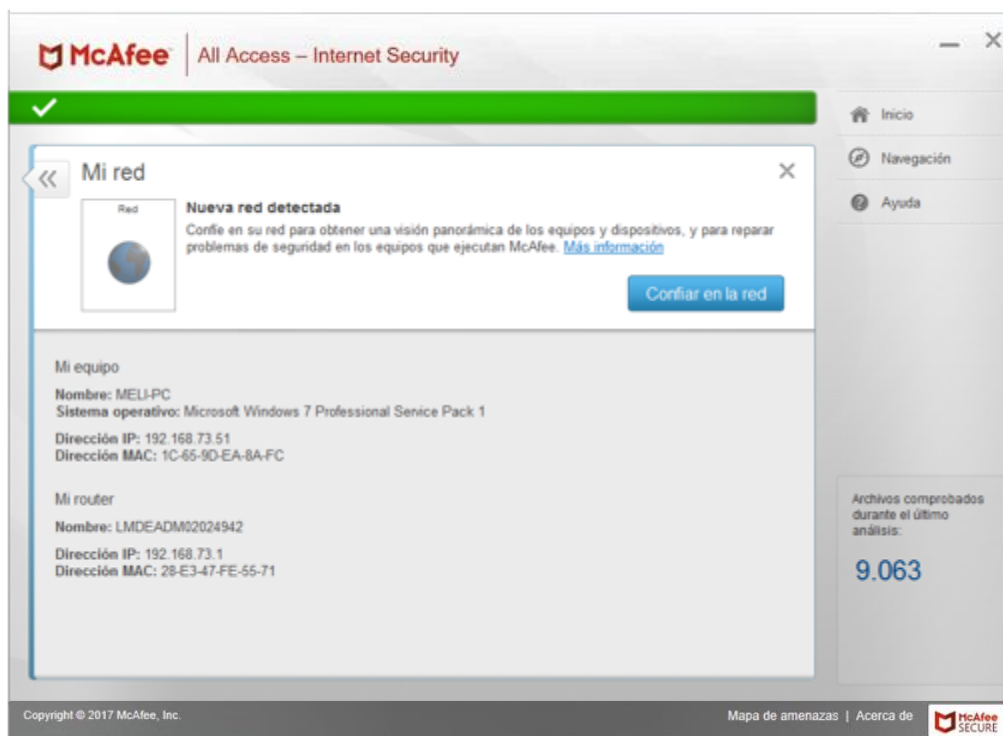


McAfee permite hacer una protección a la red doméstica. Ofrece una visión general de equipos y dispositivos de red y le permite reparar problemas de seguridad en equipos con McAfee.



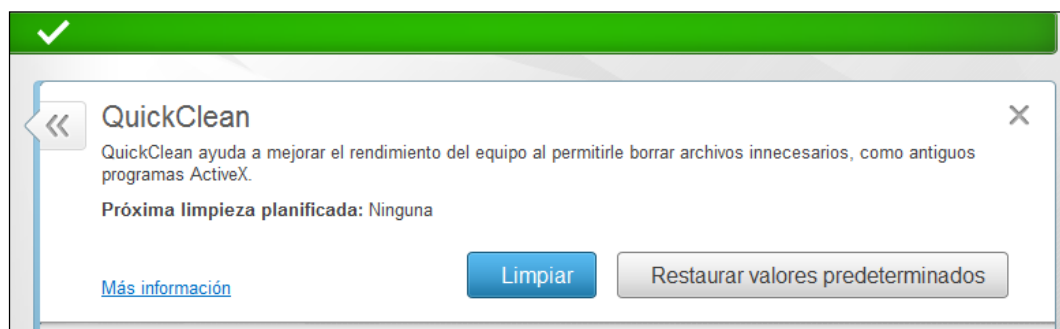
1.1.6.1 Mi red Doméstica:

Ofrece una visión general de equipos y dispositivos en la red y le permite reparar problemas de seguridad en equipos con McAfee.



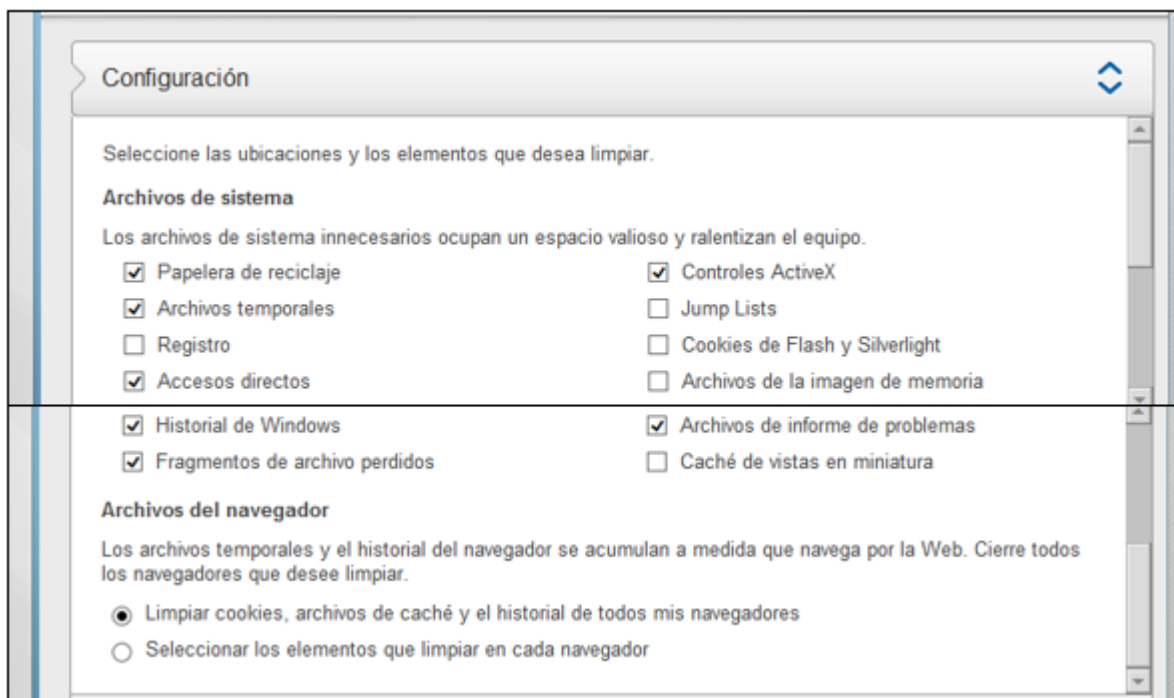
1.1.6.2 QuickClean:

Ayuda a mejorar el rendimiento del equipo al permitirle borrar archivos innecesarios.



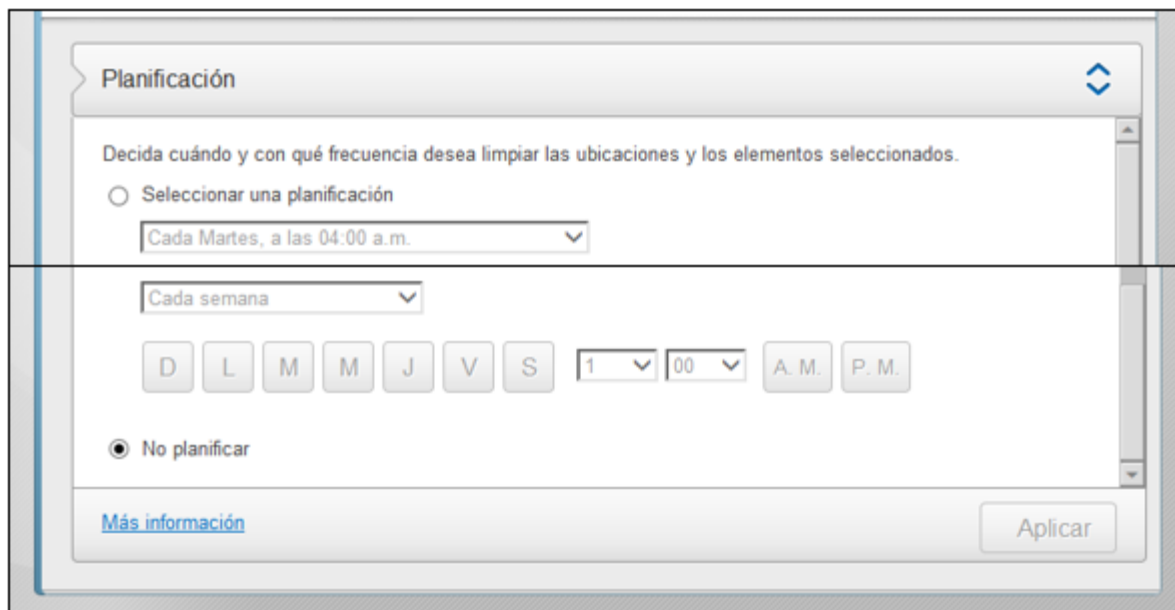
1.1.6.2.1 Configuración

Permite seleccionar las ubicaciones y los elementos que desea limpiar.



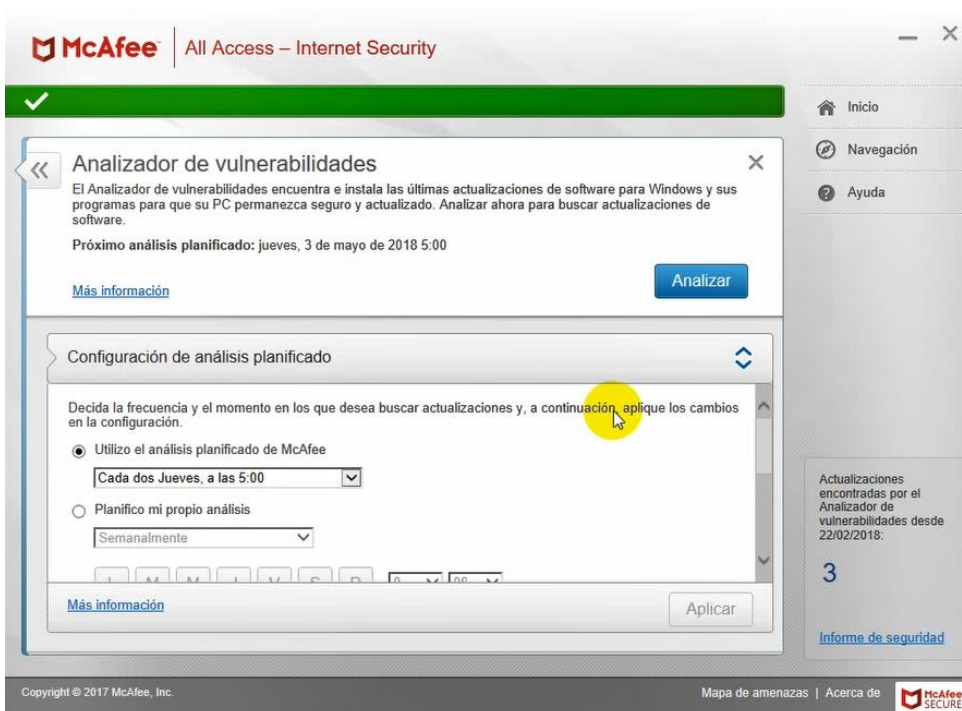
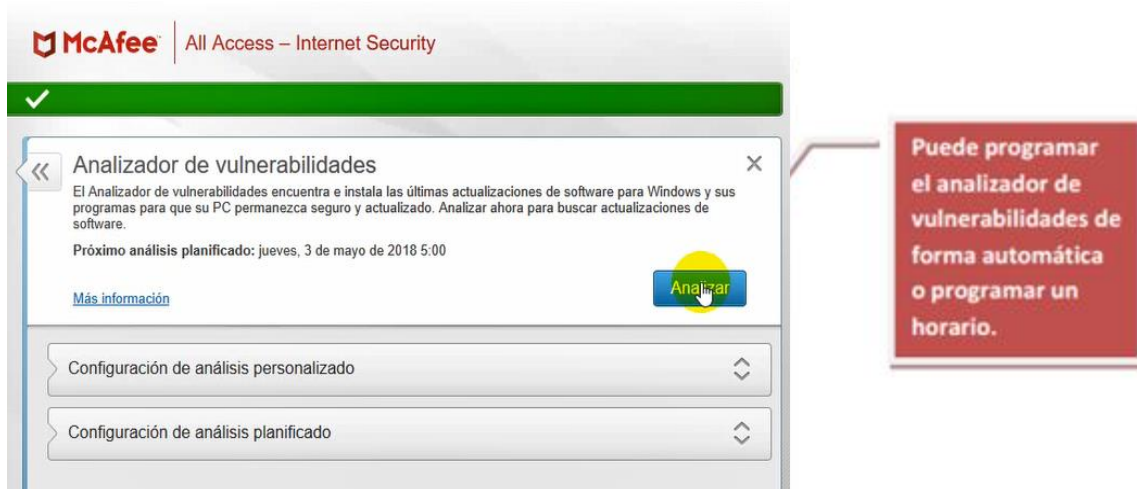
1.1.6.2.2 Planificación

Permite seleccionar la frecuencia en que se desea limpiar los elementos seleccionados.



1.1.6.3 Analizador de vulnerabilidades

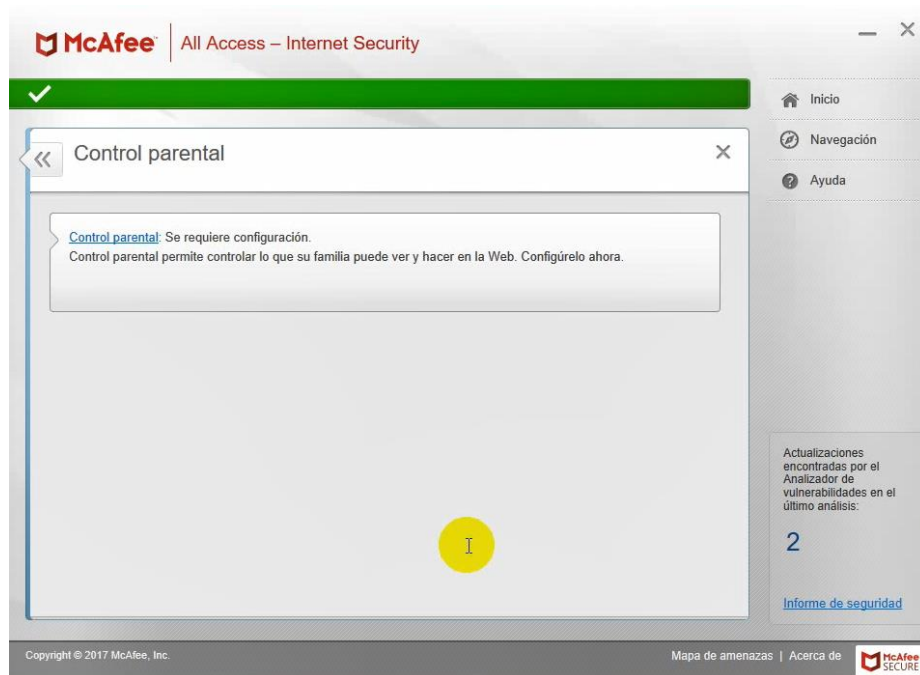
El analizador de vulnerabilidades encuentra e instala las últimas actualizaciones de software para que su equipo permanezca seguro y actualizado.



1.1.7 Control parental

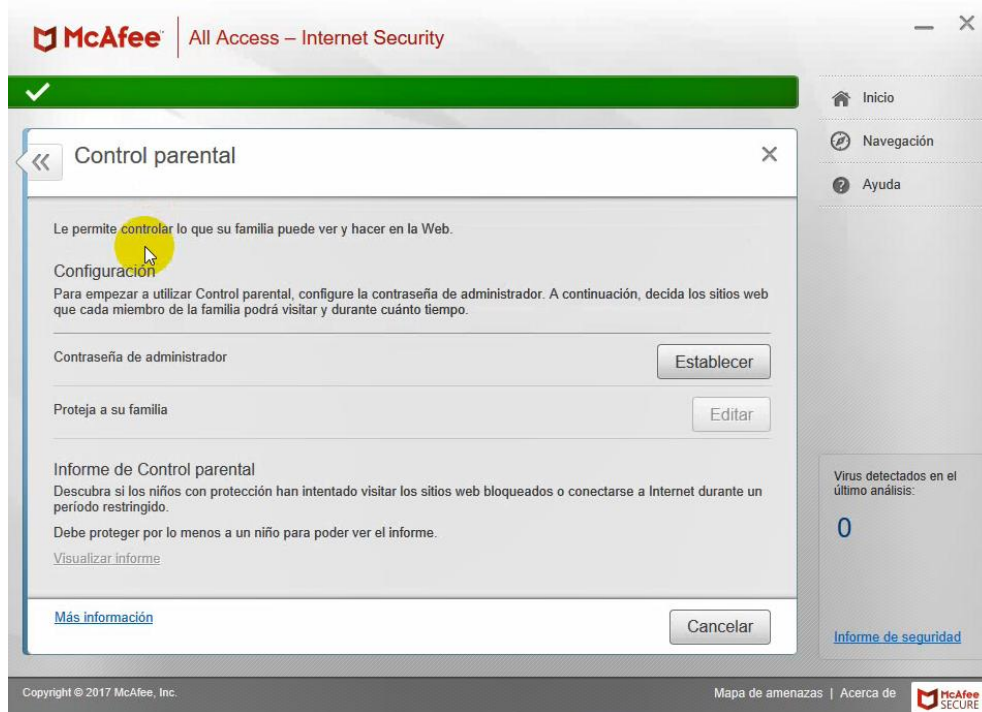


El componente Control Parental proporciona un nivel de protección de gran fiabilidad para que su familia navegue con seguridad, teniendo control total de lo que ven y puedan hacer en la web.



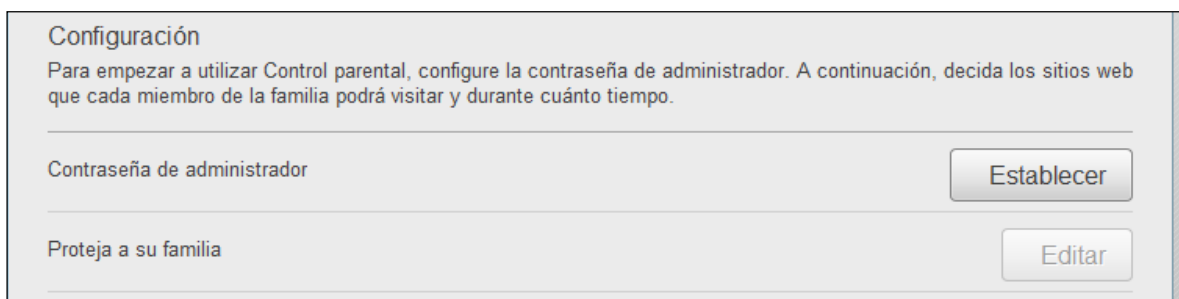
1.1.7.1 Configuración de Control parental:

Antes de poder proteger a su familia, debe designar una contraseña de administrador, la cual le permitirá únicamente a usted decidir lo que su familia puede ver y hacer en la web.

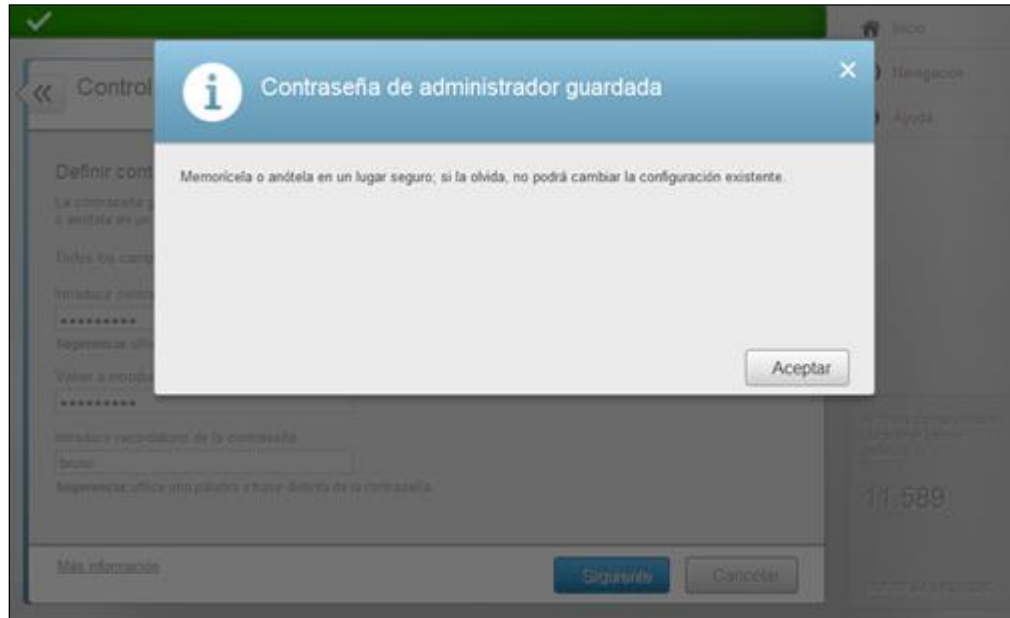


1.1.7.1.1 Definir contraseña de administrador:

Para asignar la contraseña de administrador, ingresamos desde el panel de inicio al componente *Control parental* (1) y luego en *Configurar* (2). Luego, frente a *Contraseña de administrador*, marcamos la opción *Establecer*.



Ingresamos la contraseña (3) utilizando únicamente números y letras, las mayúsculas son tenidas en cuenta. Reconfirmamos la contraseña introduciéndola nuevamente (4). Finalmente introducimos una palabra o frase distinta a la contraseña, que nos recuerde la contraseña que asignamos. Marcamos *Siguiente*.



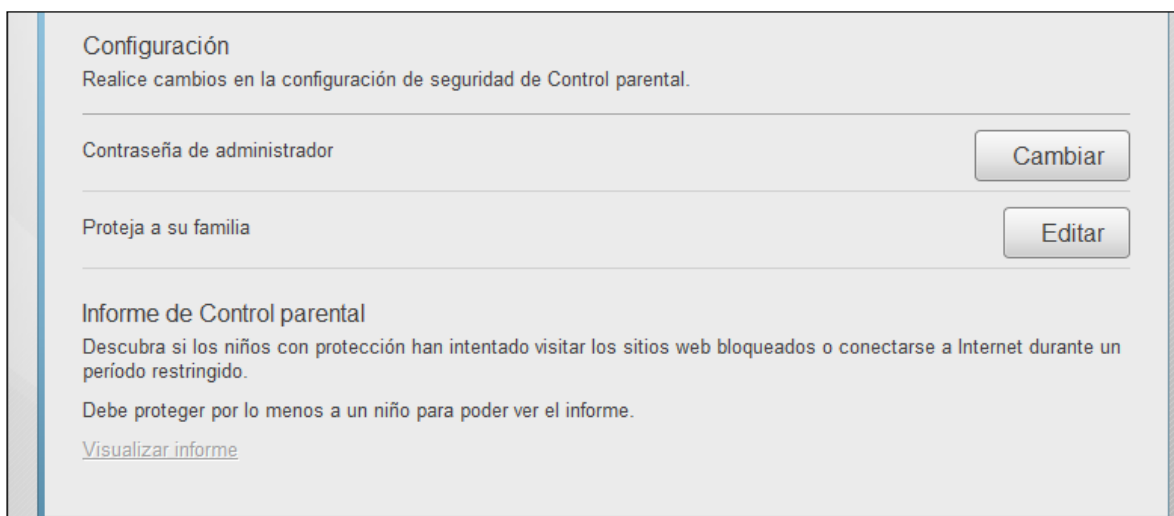
Si olvida la contraseña de administrador una vez asignada no podrá iniciar sesión en el Control parental. Asegúrese de memorizarla, o de apuntarla y guardarla en un lugar seguro; de lo contrario tendrá que reinstalar el software de McAfee para restablecer la contraseña.

1.1.7.1.2 Protección de los usuarios:

Una vez asignada la contraseña de administrador del Control Paterna se puede empezar a configurar los parámetros de seguridad que le permitirán proteger a los miembros de su familia.

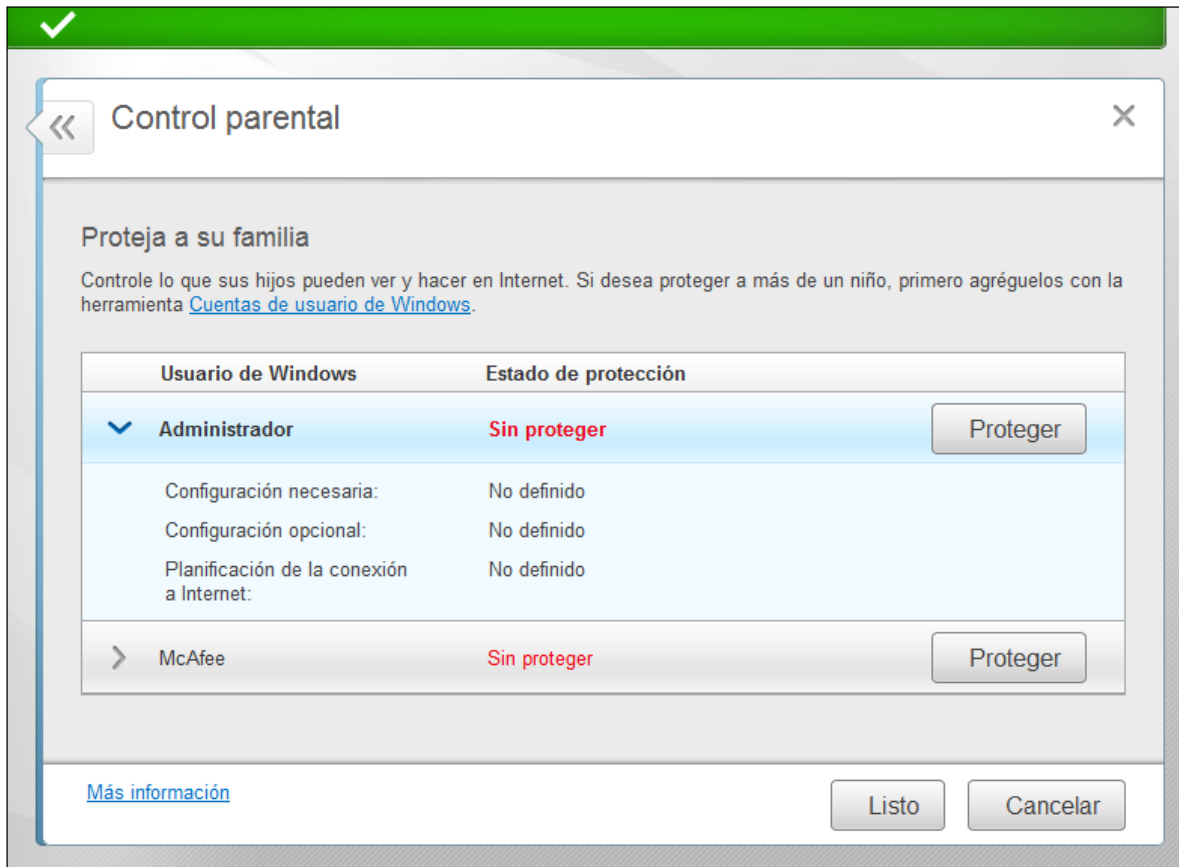
Asignación de un usuario a un grupo de edad.

En primer lugar se debe asignar al usuario un grupo de edad, permitiendo al Centro de Seguridad de McAfee saber qué contenido se considera apropiado para él. Antes de poder aplicar otros parámetros de configuración de protección, es preciso asignar al usuario a un grupo de edad. Para ello ingrese desde el panel de inicio al componente *Control parental* (1) y luego en *Configurar* (2), a continuación marque *Editar* en la opción *Proteja a su familia* (7)



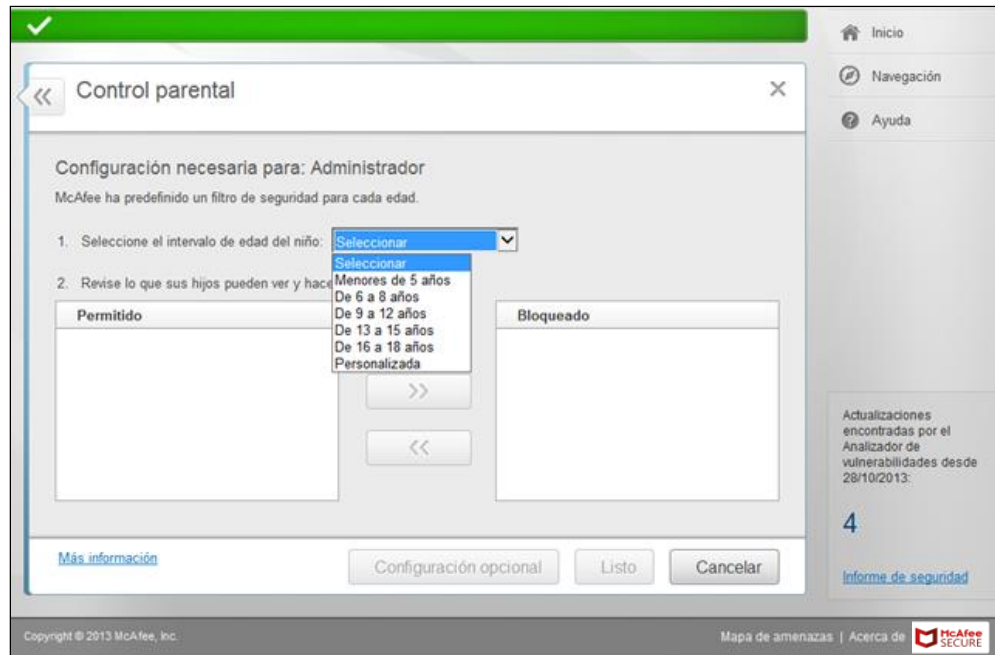
The screenshot shows the 'Configuración' (Configuration) window for McAfee Control Parental. It has a light gray background with a blue vertical bar on the left. The title 'Configuración' is at the top left. Below it is the subtitle 'Realice cambios en la configuración de seguridad de Control parental.' (Make changes to the security configuration of Control Parental). There are two main sections. The first section is 'Contraseña de administrador' (Administrator password) with a text input field and a 'Cambiar' (Change) button to its right. The second section is 'Proteja a su familia' (Protect your family) with a text input field and an 'Editar' (Edit) button to its right. Below these sections is the 'Informe de Control parental' (Control Parental Report) section. It contains the text: 'Descubra si los niños con protección han intentado visitar los sitios web bloqueados o conectarse a Internet durante un período restringido.' (Discover if children with protection have attempted to visit blocked websites or connect to the Internet during a restricted period.) and 'Debe proteger por lo menos a un niño para poder ver el informe.' (You must protect at least one child to be able to view the report.). At the bottom of this section is a link that says 'Visualizar informe' (View report).

Ingrese la contraseña de administrador y presione *Enter*. Los usuarios que aparecen a continuación son las mismas cuentas de usuario de Windows que se definieron previamente en el equipo. (Para verificar como se crean usuarios en Windows)



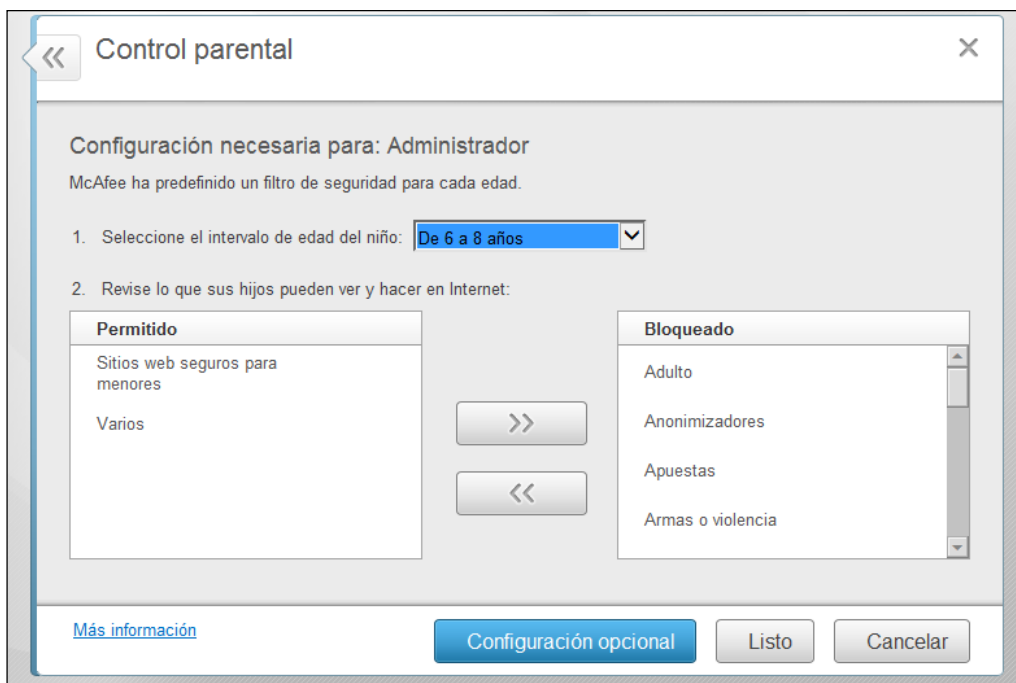
Si agrega un usuario mediante el Panel de control, Cuentas de usuario, debe cerrar el Centro de Seguridad de McAfee y, a continuación, al volverlo abrir podrá asignarle valores de configuración de protección en Control parental.

Para continuar, frente al usuario deseado, marque *Proteger*. Ahora se puede seleccionar un rango de edad de que sea apropiado para el usuario.



1.1.7.1.3 Definición de una categoría de contenido como autorizada:

Después de asignar al usuario un grupo de edad, el Centro de Seguridad de McAfee autorizará una categoría de contenido al usuario, permitiendo el acceso de éste a sitios web que contengan contenido apropiado de acuerdo al grupo de edad escogido. Se selecciona el grupo de edad de 9 a 12 años se encuentran las siguientes categorías de sitios *Permitidos* y *Bloqueados*.



Estos listados pueden personalizarse, agregando o quitando categorías, tanto en *Permitidos* y *Bloqueados*. Es posible quitar *Juegos de Permitido*, se selecciona esta categoría y se presiona el botón que apunta a *Bloqueado* (8).

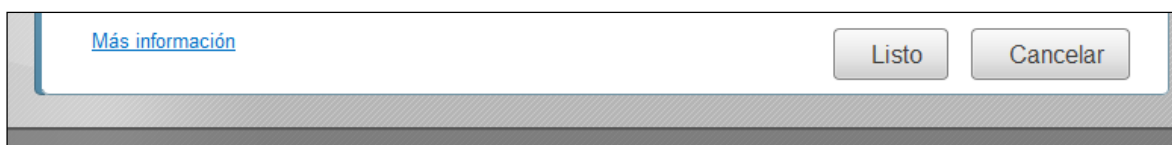


Si efectúa algún cambio en las listas *Permitido* y *Bloqueado* correspondientes a un grupo de edad específico, éste cambiará automáticamente a *Personalizado*.

1.1.7.1.4 Uso de la búsqueda segura:

Algunos motores de búsqueda, como Google, Bing o Yahoo ofrecen funciones de búsqueda segura, una configuración que descarta de la lista de resultados de búsqueda de un usuario los vínculos o el contenido potencialmente inapropiado. Por lo general, estos motores de búsqueda permiten elegir el grado de restricción que se desea aplicar al filtro de búsqueda segura, pero también autorizan a cualquier usuario a desactivar esta función en todo momento.

Una vez asignada una categoría de contenido como autorizada, continuamos con *Configuración opcional* (9).

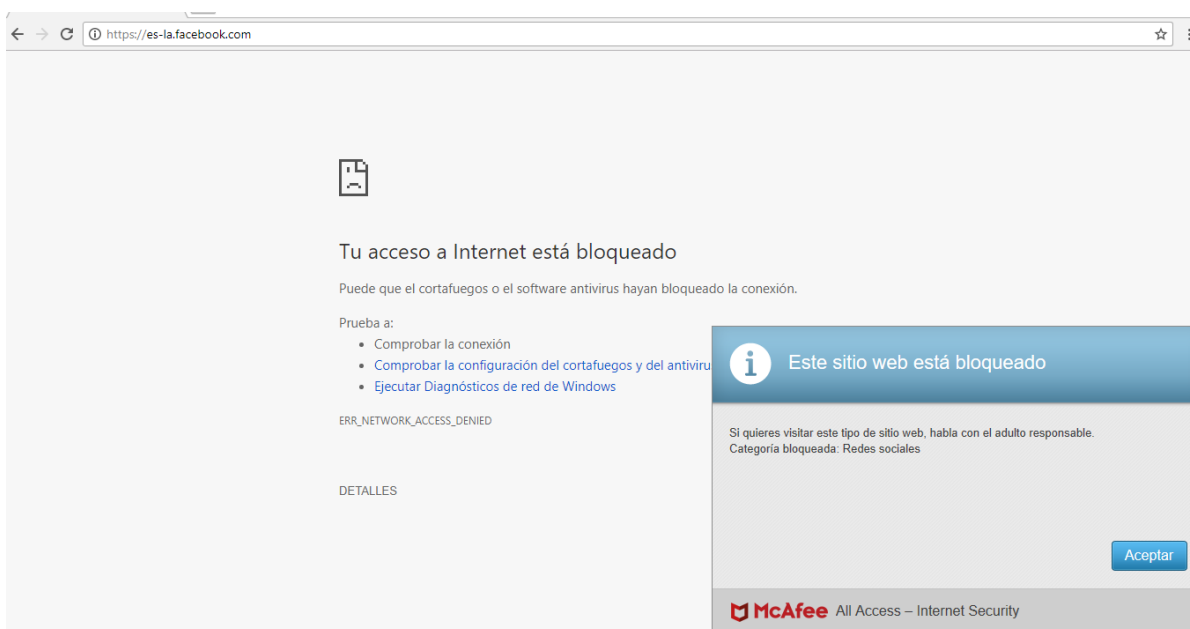


Con el Control parental, la búsqueda segura se activa de forma predeterminada cuando configuramos la protección de los usuarios.

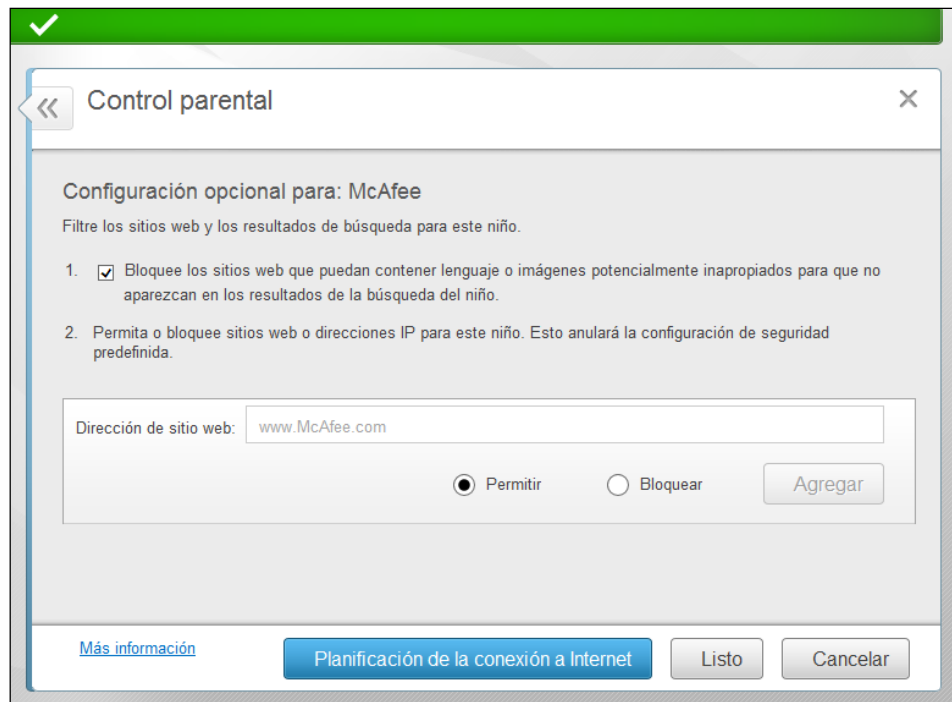


1.1.7.1.5 Autorizar y bloquear sitios web:

Si un usuario visita un sitio Web bloqueado, aparecerá un mensaje que informa de que McAfee ha bloqueado dicho sitio:

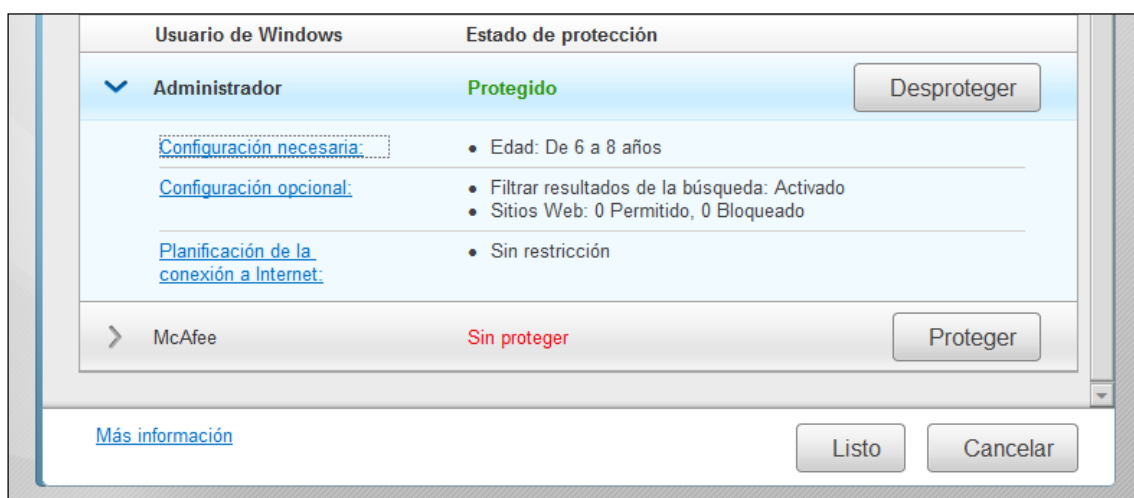


Si desea que un usuario pueda visitar un sitio web específico, puede agregar la dirección web correspondiente en la lista de filtros (10) y definir el nivel de permiso como *Permitir* (11) y *Agregar* (13). Si, por el contrario, no desea que el usuario tenga acceso a un sitio web específico, puede agregar la dirección web correspondiente en la lista de filtros (10) y definir el nivel de permiso como *Bloquear* (12) y *Agregar* (13).




Los sitios web y los permisos que se incorporen a esta lista, tanto como sitios permitidos y bloqueados, anularán los permisos definidos por grupos de edad y categorías de contenido.

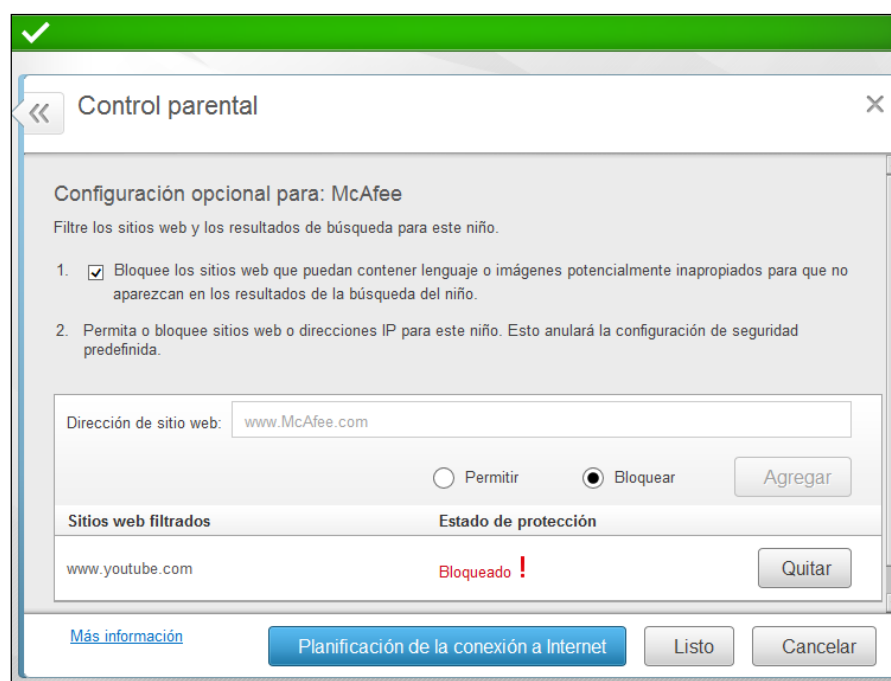
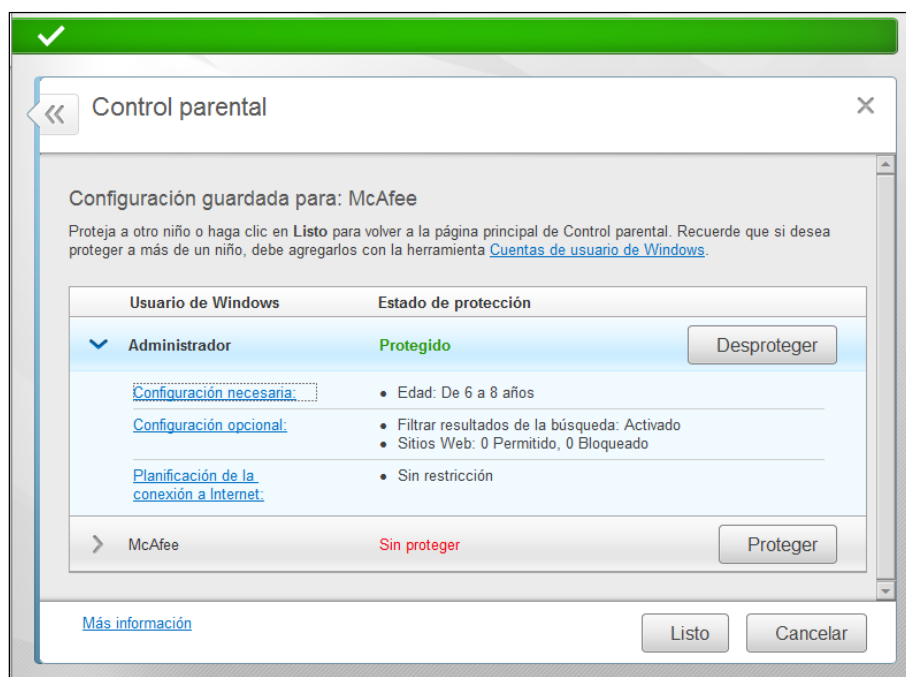
Si desea que el *Control Parental* deje de filtrar un sitio Web específico, puede eliminarlo en cualquier momento, presionando *Quitar*.



Usuario de Windows	Estado de protección	Acción
Administrador	Protegido	Desproteger
<u>Configuración necesaria:</u> - Edad: De 6 a 8 años <u>Configuración opcional:</u> - Filtrar resultados de la búsqueda: Activado - Sitios Web: 0 Permitido, 0 Bloqueado <u>Planificación de la conexión a Internet:</u> - Sin restricción		
McAfee	Sin proteger	Proteger

1.1.7.1.6 Control del tiempo de navegación en la web:

De forma predeterminada, todos los usuarios podrán navegar por Internet cuando deseen. Sin embargo, si le preocupa que un usuario dedique demasiado tiempo a navegar por la web, podrá controlar el acceso a ésta y establecer un límite de tiempo para ello. Para ello, continuamos la configuración del *Control Parental*, presionando *Planificación de la navegación Web* (14)



Control parental

Planificación de la conexión a Internet para: McAfee Consumer

Cree una planificación para asegurarse de que su hijo no pasa demasiado tiempo conectado a Internet.

☒ Permitir a mi hijo conectarse a Internet cuando desee.

☐ Deseo elegir cuándo se puede conectar a Internet mi hijo.

	Dom	Lu	Mar	Mié	Jue	Vie	Sáb
00:00							
01:00							
02:00							
03:00							

[Más información](#)

Listo Cancelar

Si está en verde indicará el tiempo permitido, si está en color blanco indicará el tiempo bloqueado

Ya no puedes conectarte a Internet

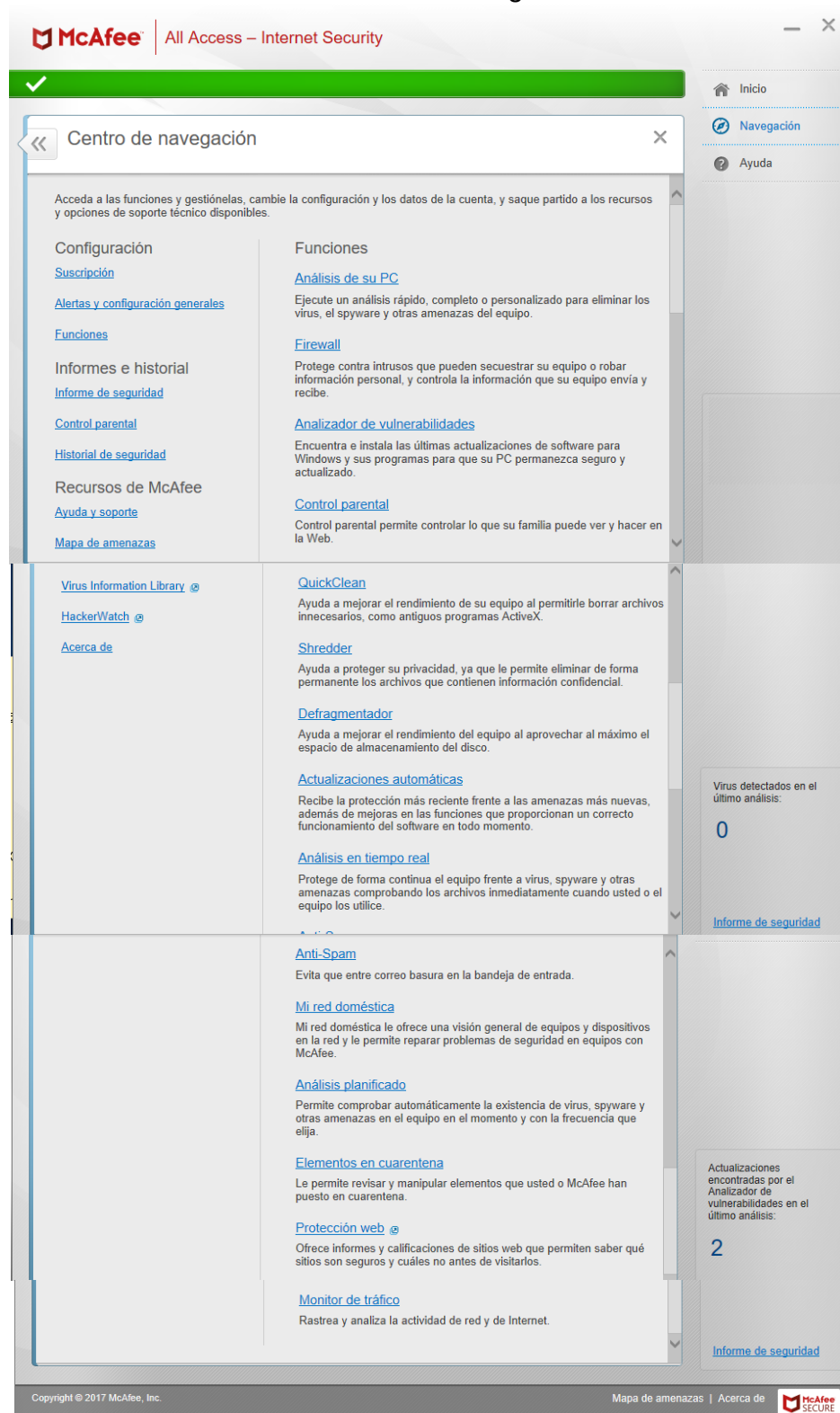
Tus padres han definido una planificación de conexión a Internet en Control parental. Si crees que hay un error, puedes pedirles que cambien la configuración.

Aceptar

McAfee All Access – Internet Security

2. Centro de navegación:

Contiene el acceso a las funciones donde se configura la información de cuenta.



McAfee All Access – Internet Security

Centro de navegación

Acceda a las funciones y gestiónelas, cambie la configuración y los datos de la cuenta, y saque partido a los recursos y opciones de soporte técnico disponibles.

Configuración

- [Suscripción](#)
- [Alertas y configuración generales](#)

Funciones

- [Análisis de su PC](#)
Ejecute un análisis rápido, completo o personalizado para eliminar los virus, el spyware y otras amenazas del equipo.
- [Firewall](#)
Protege contra intrusos que pueden secuestrar su equipo o robar información personal, y controla la información que su equipo envía y recibe.
- [Analizador de vulnerabilidades](#)
Encuentra e instala las últimas actualizaciones de software para Windows y sus programas para que su PC permanezca seguro y actualizado.
- [Control parental](#)
Control parental permite controlar lo que su familia puede ver y hacer en la Web.

Informes e historial

- [Informe de seguridad](#)

Recursos de McAfee

- [Ayuda y soporte](#)
- [Mapa de amenazas](#)

Virus Information Library

HackerWatch

Acerca de

QuickClean
Ayuda a mejorar el rendimiento de su equipo al permitirle borrar archivos innecesarios, como antiguos programas ActiveX.

Shredder
Ayuda a proteger su privacidad, ya que le permite eliminar de forma permanente los archivos que contienen información confidencial.

Defragmentador
Ayuda a mejorar el rendimiento del equipo al aprovechar al máximo el espacio de almacenamiento del disco.

Actualizaciones automáticas
Recibe la protección más reciente frente a las amenazas más nuevas, además de mejoras en las funciones que proporcionan un correcto funcionamiento del software en todo momento.

Análisis en tiempo real
Protege de forma continua el equipo frente a virus, spyware y otras amenazas comprobando los archivos inmediatamente cuando usted o el equipo los utilice.

Anti-Spam
Evita que entre correo basura en la bandeja de entrada.

Mi red doméstica
Mi red doméstica le ofrece una visión general de equipos y dispositivos en la red y le permite reparar problemas de seguridad en equipos con McAfee.

Análisis planificado
Permite comprobar automáticamente la existencia de virus, spyware y otras amenazas en el equipo en el momento y con la frecuencia que elija.

Elementos en cuarentena
Le permite revisar y manipular elementos que usted o McAfee han puesto en cuarentena.

Protección web
Ofrece informes y calificaciones de sitios web que permiten saber qué sitios son seguros y cuáles no antes de visitarlos.

Monitor de tráfico
Rastrea y analiza la actividad de red y de Internet.

Virus detectados en el último análisis:
0

Actualizaciones encontradas por el Analizador de vulnerabilidades en el último análisis:
2

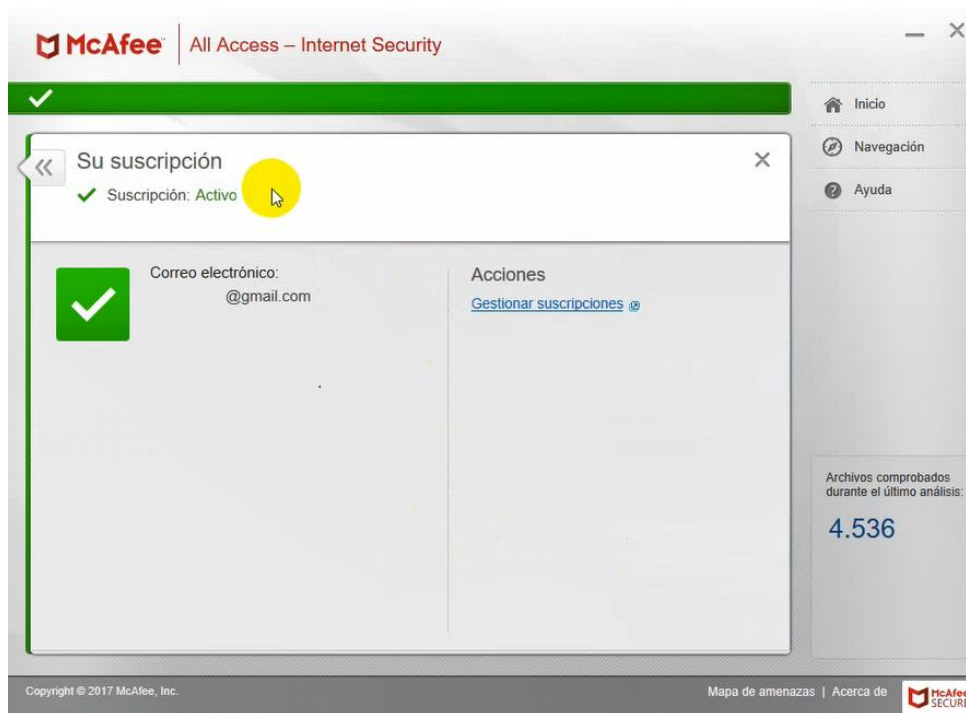
Copyright © 2017 McAfee, Inc. Mapa de amenazas | Acerca de McAfee SECURE

2.1 Configuración:

Permite ingresar a algunas funciones para configurar la consola.

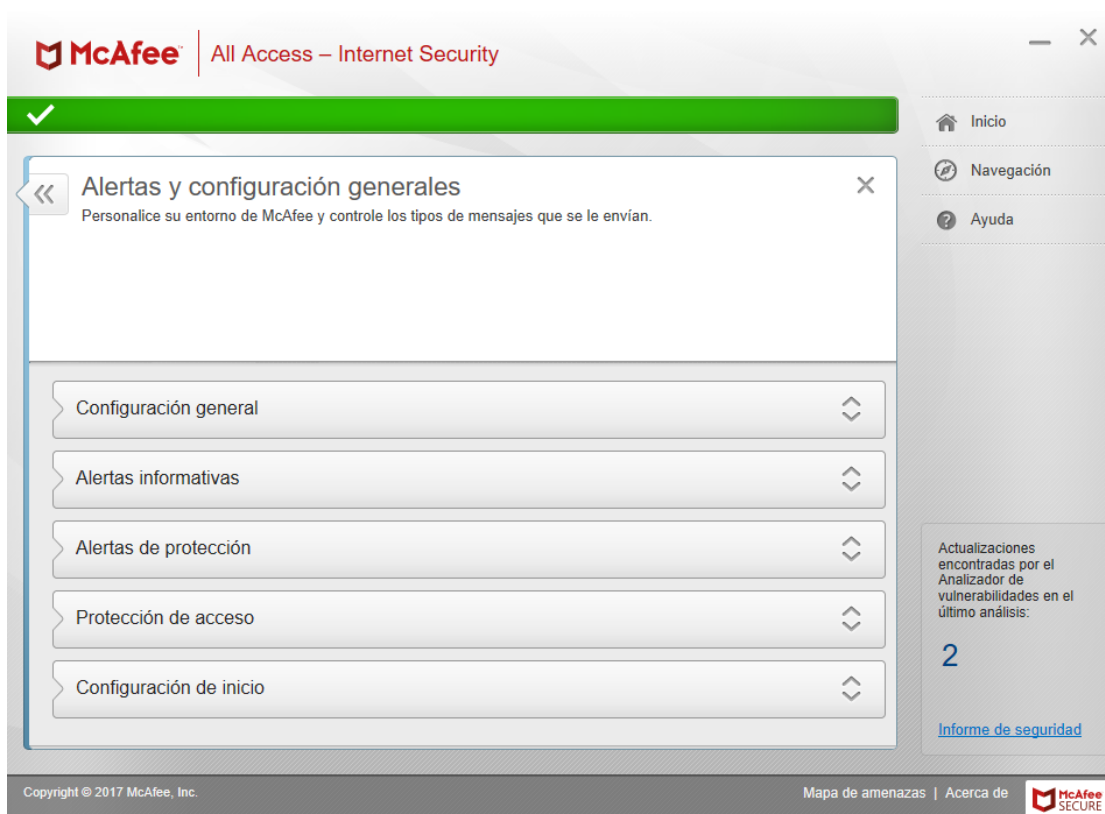
2.1.1 Suscripción:

Permite verificar el estado de la suscripción.

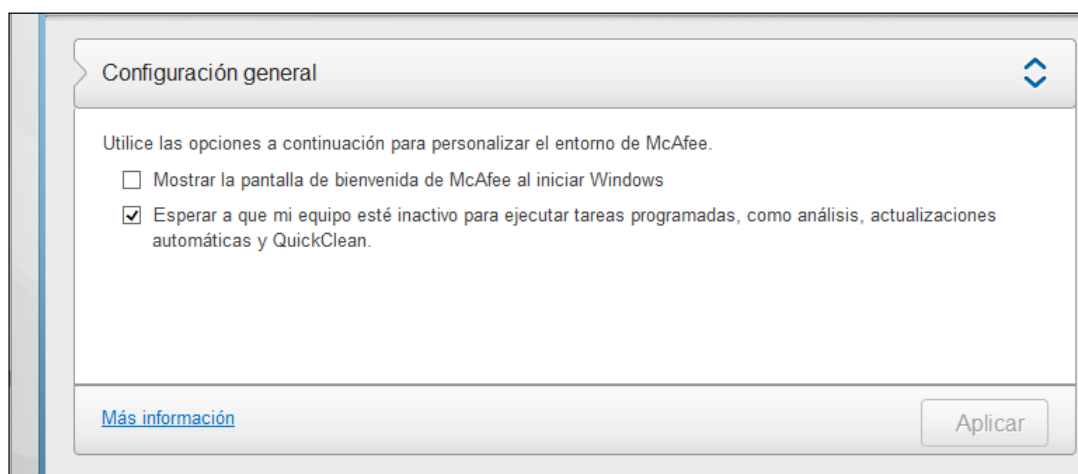


2.1.2 Alertas y configuración generales:

Permite personalizar su entorno de McAfee y controlar los tipos de mensajes que le envían.



2.1.2.1 Configuración General:



2.1.2.2 Alertas informativas:

Alertas informativas

Las alertas informativas le permiten enterarse de los eventos relacionados con el estado de la protección.

☒ Mostrar alertas informativas cuando:

☐ Se permite que un programa se conecte a Internet.

☒ La actualización manual se está ejecutando en segundo plano.

[Más información](#)

Aplicar

2.1.2.3 Alertas de protección:

Alertas de protección

McAfee siempre le permitirá saber cuándo la configuración de seguridad y los eventos afectan al estado de la protección. Puede elegir qué alertas no desea que se muestren.

☐ No mostrar una alerta si el firewall está desactivado

[Más información](#)

Aplicar

2.1.2.4 Protección de acceso

Protección de acceso

Proteja los archivos y servicios de McAfee más importantes para que no se eliminen por accidente.

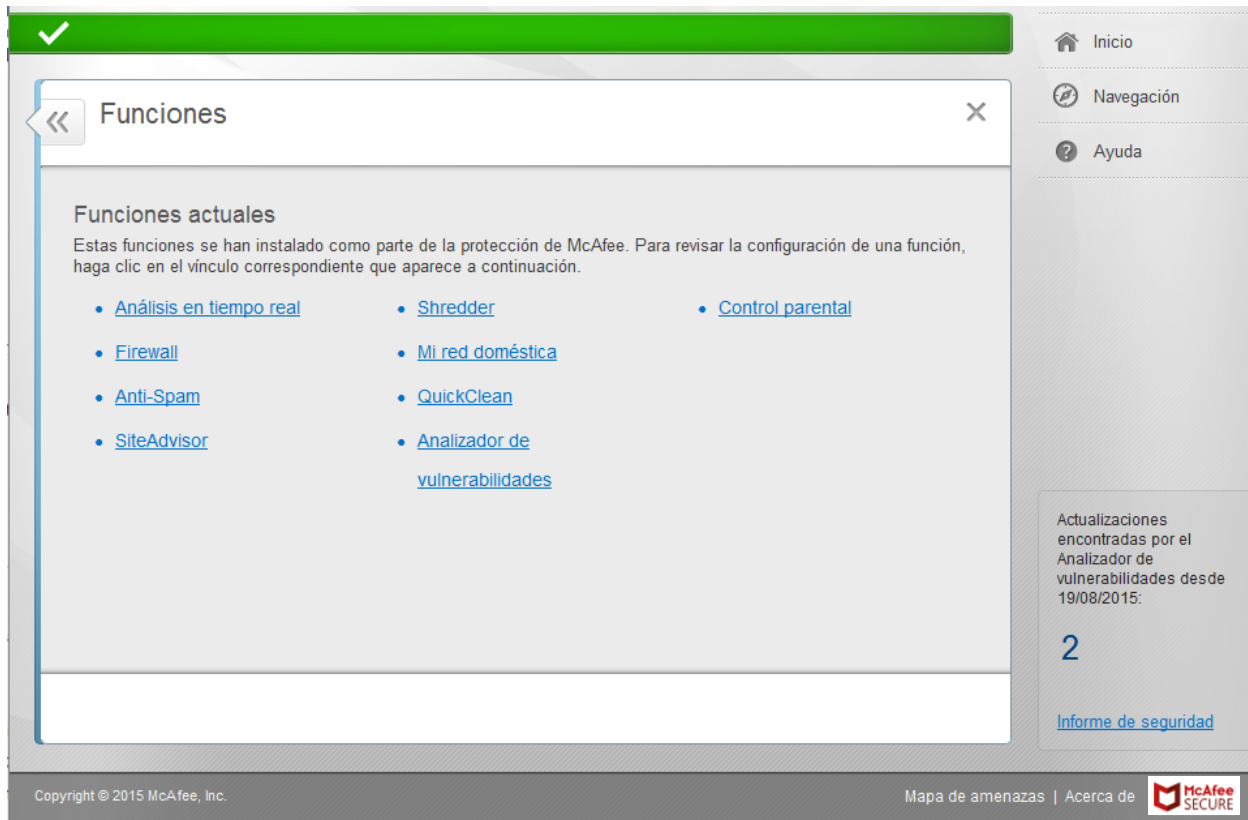
☒ Utilizar protección de acceso

[Más información](#)

Aplicar

2.1.3 Funciones:

Estas funciones se han instalado como parte de la protección de McAfee. Permite revisar la configuración de una función.



2.2 Informes e historial:

Permite visualizar los últimos resultados acerca de los análisis e imprimirlos.

2.2.1 Informe de seguridad:

Permite ver los últimos resultados de los análisis y permite imprimir el informe.




McAfee™ All Access – Internet Security

Descripción general

Actividad total

Control parental

lunes, 03 de agosto de 2015

A continuación, encontrará un resumen de la actividad en su equipo desde que instaló McAfee.

Anti-Virus y Anti-Spyware

Análisis ejecutados

Rápido: 0	Desde el menú que aparece al hacer clic con el botón secundario del ratón: 0
Completo: 0	Unidad de medios extraíbles: 0
Personalizado: 0	En el reinicio: 0
Planificado: 0	

Amenazas detectadas

Virus: 0	Vulnerabilidades por desbordamiento del búfer: 0
Troyanos: 0	Programas potencialmente no deseados: 0
Rootkits: 0	

Elementos eliminados

Papelera de reciclaje: 0	Internet Explorer: 0
Archivos temporales: 0	Firefox: 0
Registro: 0	Chrome: 0
Otros archivos de sistema: 0	Safari: 0
Outlook: 0	
Windows Mail: 0	

Shredder

Total de elementos destruidos: 0

Mi red doméstica

Intrusos detectados: 0	Problemas diagnosticados: 0
Equipos de confianza: 0	Problemas reparados: 0

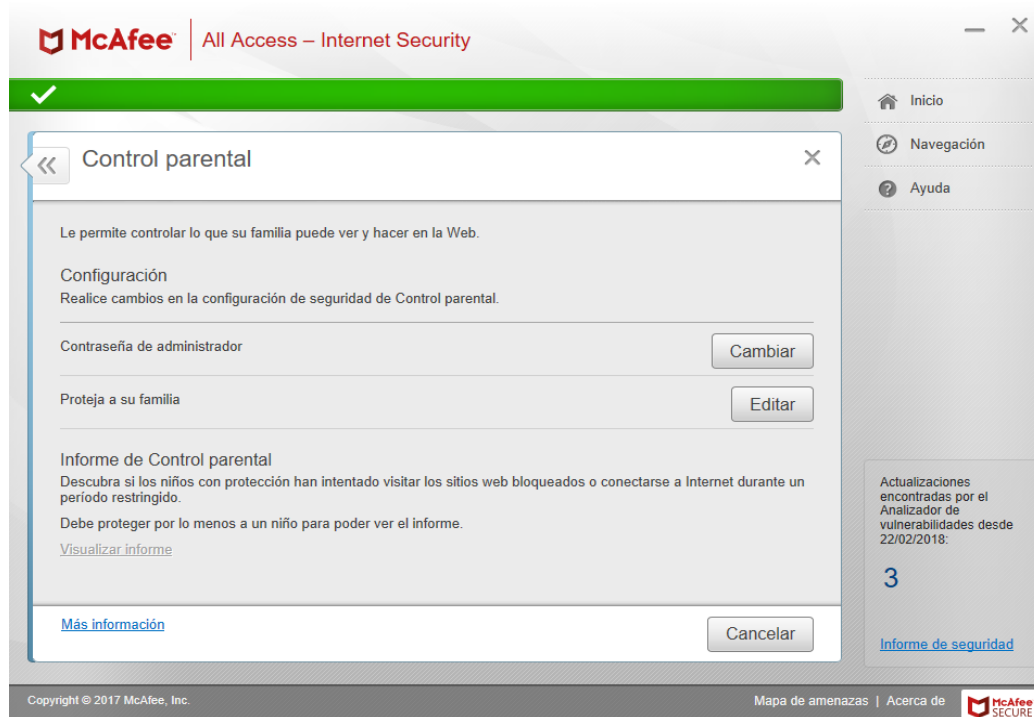
Analizador de vulnerabilidades

Aplicaciones encontradas: 4	Programas parcheados: 2
-----------------------------	-------------------------

2.2.2 Control Parental: Le permite controlar lo que su familia puede ver y hacer en la web.



Para configurar su Control Parental vaya al punto 1.1.7 de este documento.



2.2.3 Historial de seguridad:

Permite consultar el historial de seguridad y las acciones que se han realizado en el equipo:



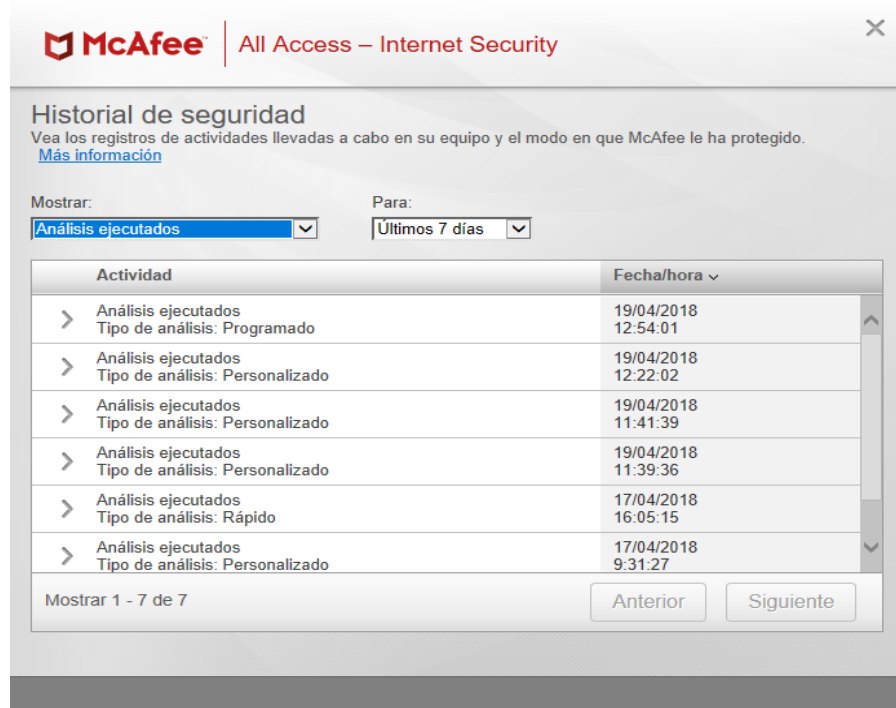
McAfee | All Access – Internet Security

Historial de seguridad
Vea los registros de actividades llevadas a cabo en su equipo y el modo en que McAfee le ha protegido.
[Más información](#)

Mostrar: Para:

Actividad	Fecha/hora
> Conexión de red entrante sospechosa bloqueada Dirección IP de origen: 52.230.10.183	23/04/2018 10:47:08
> Conexión de red entrante sospechosa bloqueada Dirección IP de origen: 216.58.222.206	23/04/2018 10:45:50
> Conexión de red entrante sospechosa bloqueada Dirección IP de origen: 216.58.222.206	23/04/2018 10:11:25
> Conexión de red entrante sospechosa bloqueada Dirección IP de origen: 169.254.144.162	23/04/2018 10:08:42
> Conexión de red entrante sospechosa bloqueada Dirección IP de origen: 169.254.144.162	23/04/2018 10:08:41
> Conexión de red entrante sospechosa bloqueada Dirección IP de origen: 169.254.144.162	23/04/2018 10:08:41

Mostrar 1 - 25 de 43



McAfee | All Access – Internet Security

Historial de seguridad
Vea los registros de actividades llevadas a cabo en su equipo y el modo en que McAfee le ha protegido.
[Más información](#)

Mostrar: Para:

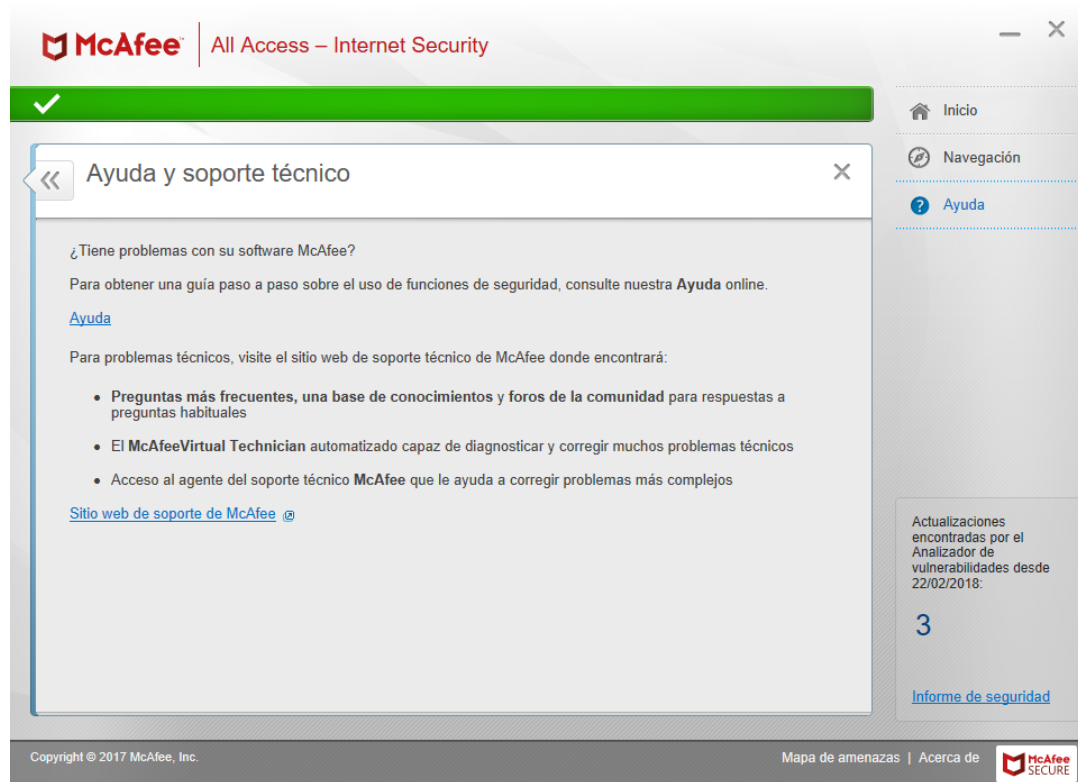
Actividad	Fecha/hora
> Análisis ejecutados Tipo de análisis: Programado	19/04/2018 12:54:01
> Análisis ejecutados Tipo de análisis: Personalizado	19/04/2018 12:22:02
> Análisis ejecutados Tipo de análisis: Personalizado	19/04/2018 11:41:39
> Análisis ejecutados Tipo de análisis: Personalizado	19/04/2018 11:39:36
> Análisis ejecutados Tipo de análisis: Rápido	17/04/2018 16:05:15
> Análisis ejecutados Tipo de análisis: Personalizado	17/04/2018 9:31:27

Mostrar 1 - 7 de 7

3. Recursos de McAfee:

3.1 Ayuda de Soporte:

A continuación seleccione el tipo de soporte que más se ajuste a sus necesidades.



Se le recomienda consultar a su operador de confianza cualquier inquietud que esta guía y/o centro de navegación le genere.

3.2 Mapa de amenazas:

Permite Visualizar las amenazas activas en su región y en todo el mundo.



McAfee All Access – Internet Security

Mapa de amenazas

El mapa de amenazas muestra las amenazas activas en su región y en todo el mundo. [Obtener más información](#)

Mostrar: **Malware**

Última actualización: 03/08/2015 19:24 UTC

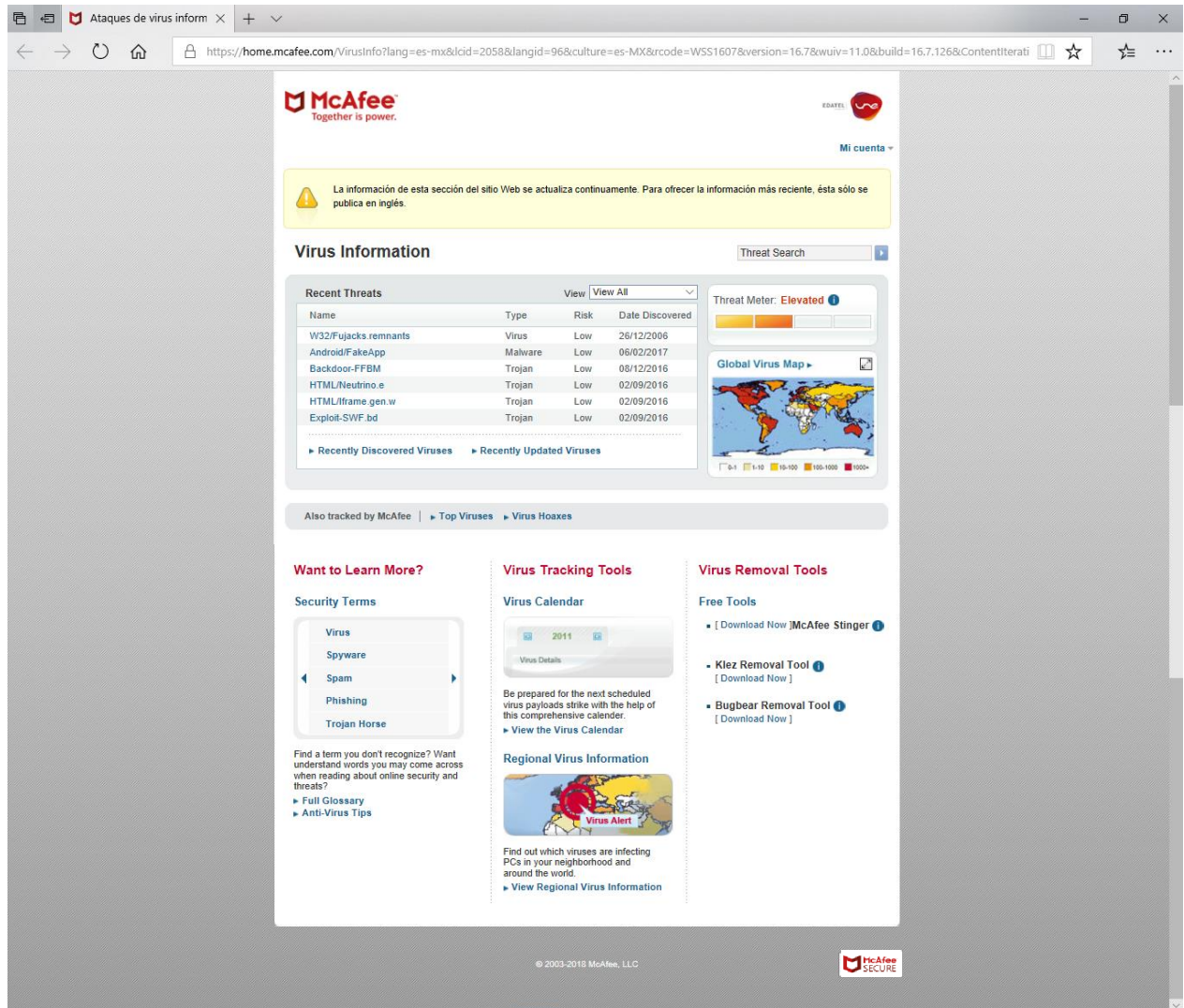
Archivos comprobados durante el último análisis: **4.675**

Alta
Moderada
Baja

Copyright © 2015 McAfee, Inc. Mapa de amenazas | Acerca de McAfee SECURE

3.3 Virus information Library:

Permite al usuario tener acceso a páginas que suministran información sobre virus.



The screenshot shows the McAfee Virus Information Library website. The page features a header with the McAfee logo and a navigation bar. A yellow warning box states: "La información de esta sección del sitio Web se actualiza continuamente. Para ofrecer la información más reciente, ésta sólo se publica en inglés." Below this, the "Virus Information" section includes a "Threat Search" bar and a "Recent Threats" table.

Name	Type	Risk	Date Discovered
W32/Fujacks remnants	Virus	Low	26/12/2006
AndroidFakeApp	Malware	Low	06/02/2017
Backdoor-FFBM	Trojan	Low	08/12/2016
HTML/Neutrino.e	Trojan	Low	02/09/2016
HTML/iframe.gen.w	Trojan	Low	02/09/2016
Exploit-SWF.bd	Trojan	Low	02/09/2016

Below the table are links for "Recently Discovered Viruses" and "Recently Updated Viruses". To the right, there is a "Threat Meter" showing an "Elevated" risk level and a "Global Virus Map".

The bottom section of the page is divided into three columns: "Want to Learn More?" (with links to Security Terms, Virus, Spyware, Spam, Phishing, and Trojan Horse), "Virus Tracking Tools" (with a Virus Calendar and Regional Virus Information), and "Virus Removal Tools" (with links to Download Now McAfee Stinger, Klez Removal Tool, and Bugbear Removal Tool).

At the bottom, there is a copyright notice: "© 2003-2018 McAfee, LLC" and the McAfee SECURE logo.

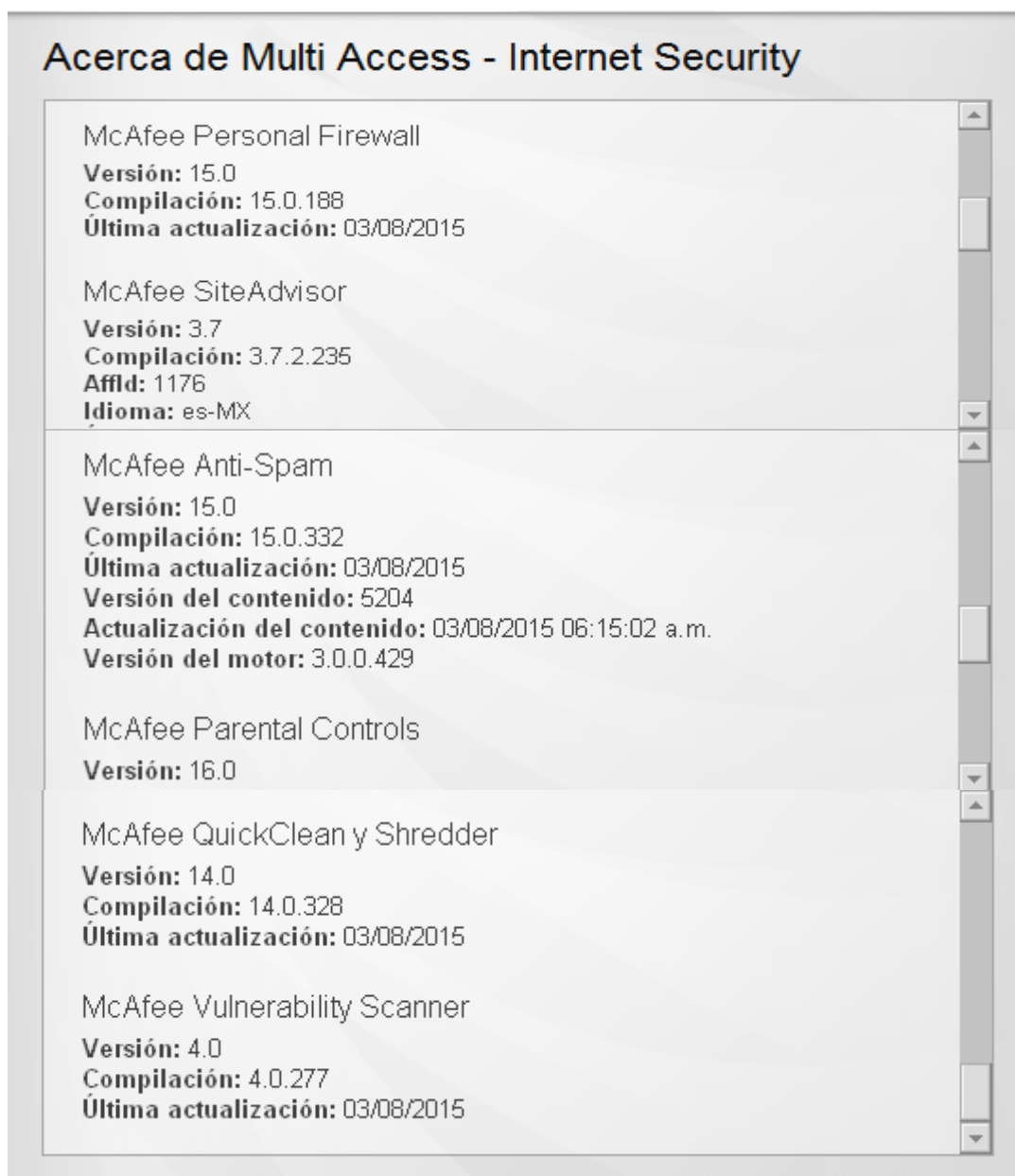
3.4 HackerWatch:

Permite informar y compartir información que ayuda a identificar, combatir y evitar la propagación de amenazas de Internet, así como el tráfico de red no deseado.



3.5 Acerca de





Para más información puede visitar

<http://download.mcafee.com/products/webhelp/4/1034/>

Muchas gracias por la oportunidad que le brinda a McAfee de proteger lo que usted más valora.