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

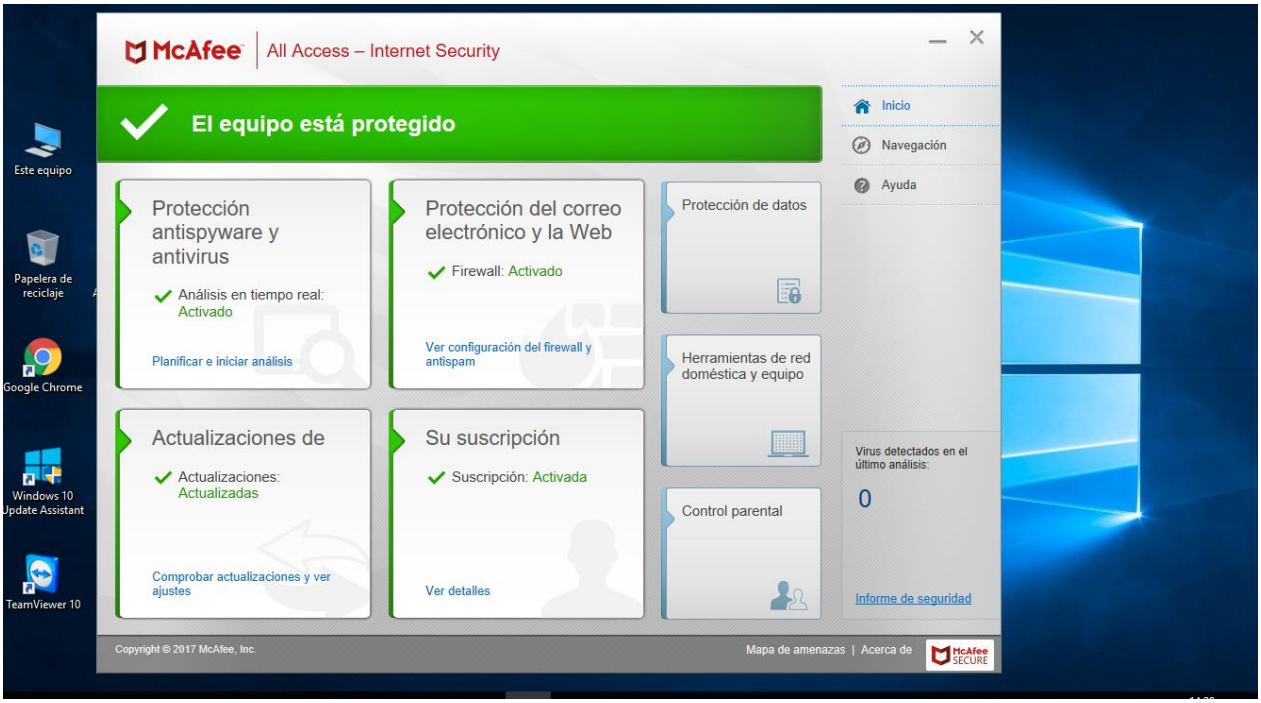
Contenido:

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.

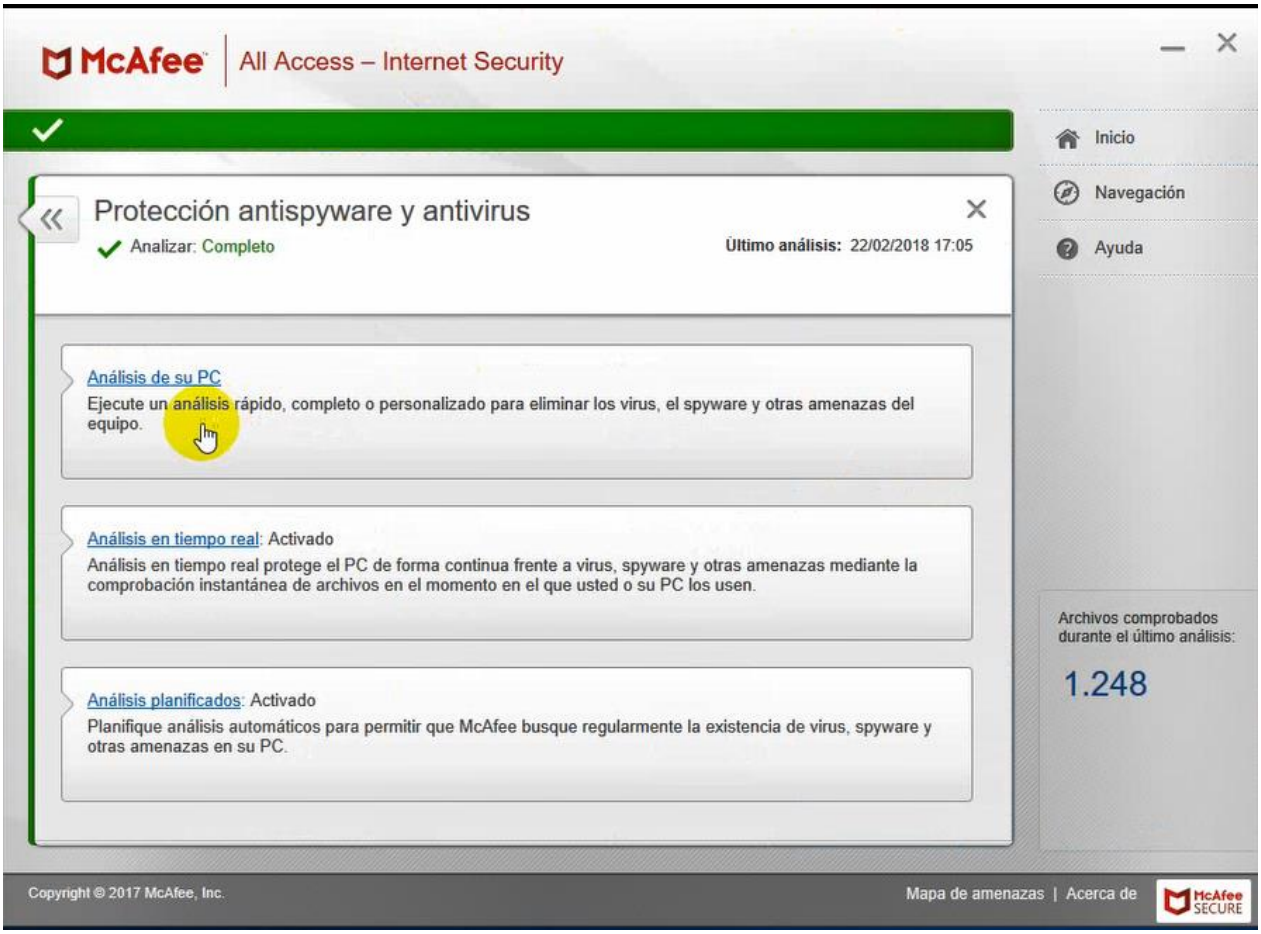
Esta guía ilustrada está basada en la consola de McAfee Multi Access – Internet Security **Versión 14.0** para consultar la versión de su consola ingrese a la sección **“Centro de navegación” “recurso de McAfee”“Acerca de”**

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.

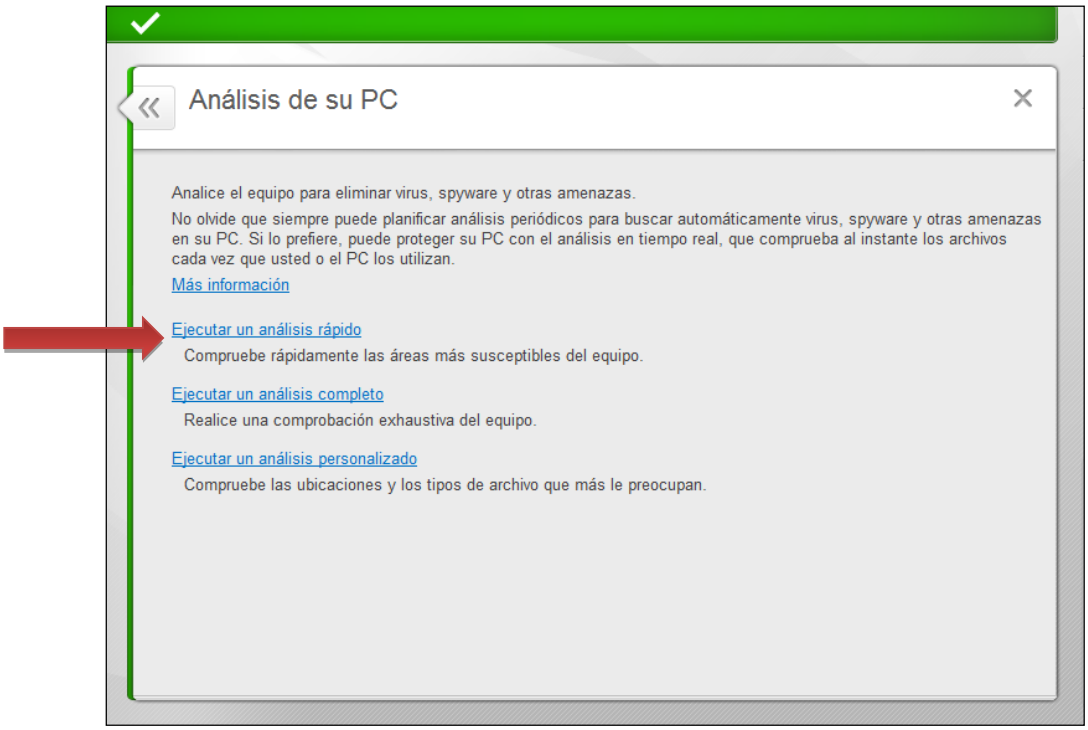
1.1.1.1 Análisis de su PC:

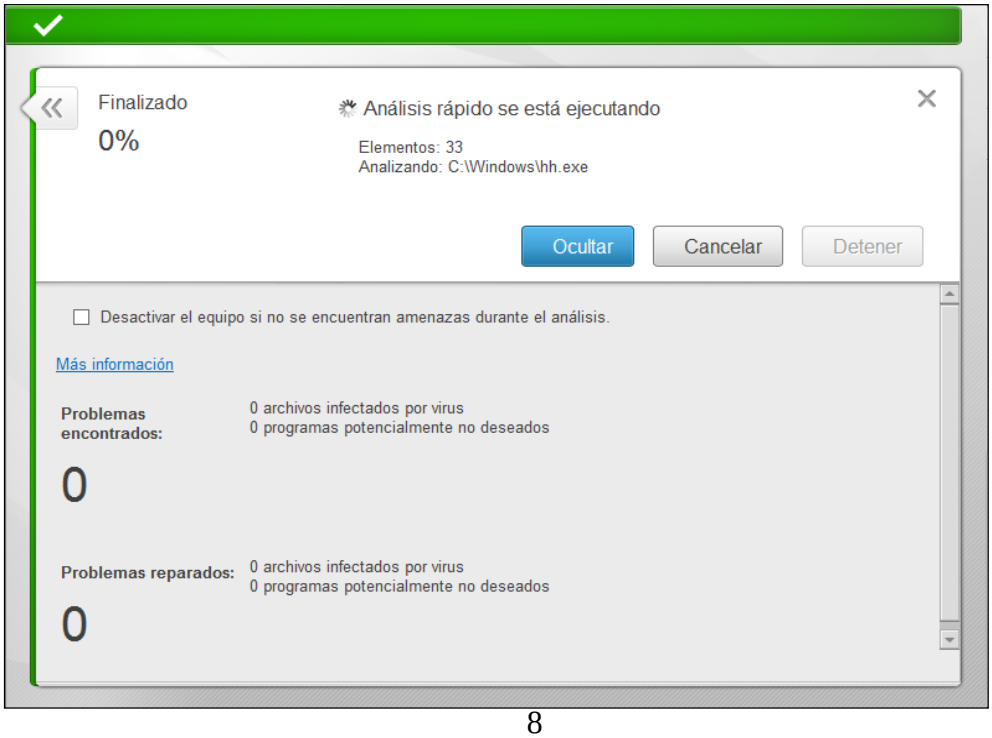
En función de sus necesidades de seguridad, puede elegir entre muchas opciones de análisis en Anti-Virus y Anti-Spyware, incluidos el análisis rápido, el análisis completo, el análisis personalizado y análisis manual. El tipo de análisis se selecciona en el Panel de inicio de McAfee, *Protección de antispyware 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:

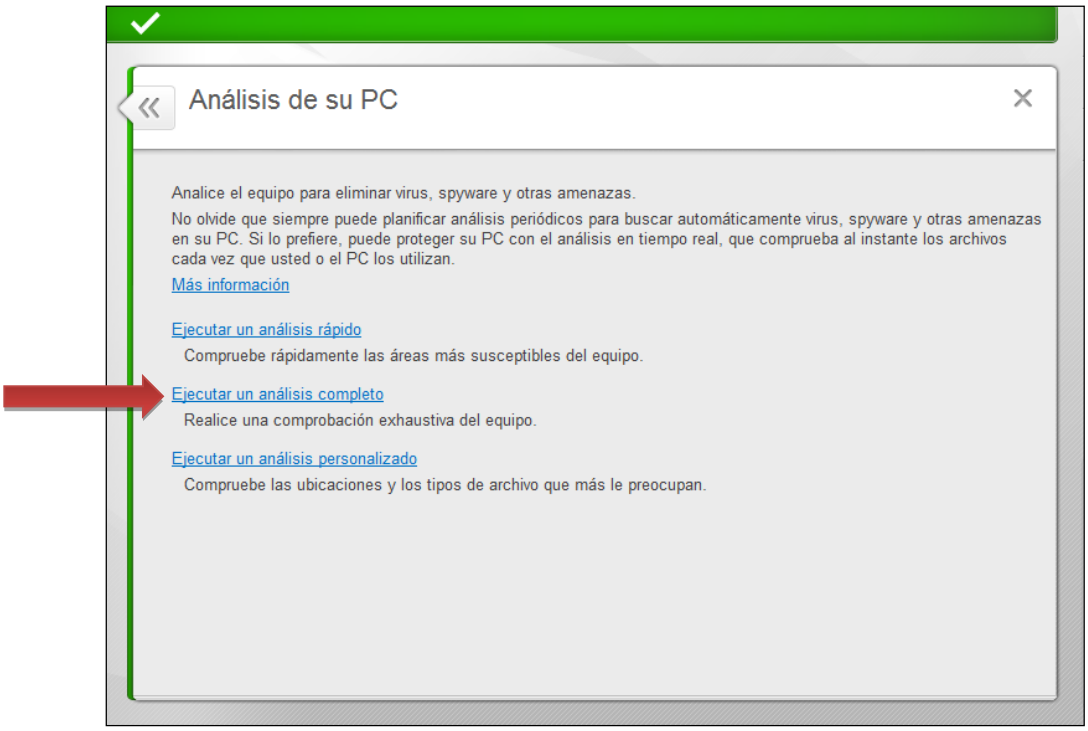
Este tipo de análisis permite verificar rápidamente las áreas más vulnerables de su computador.

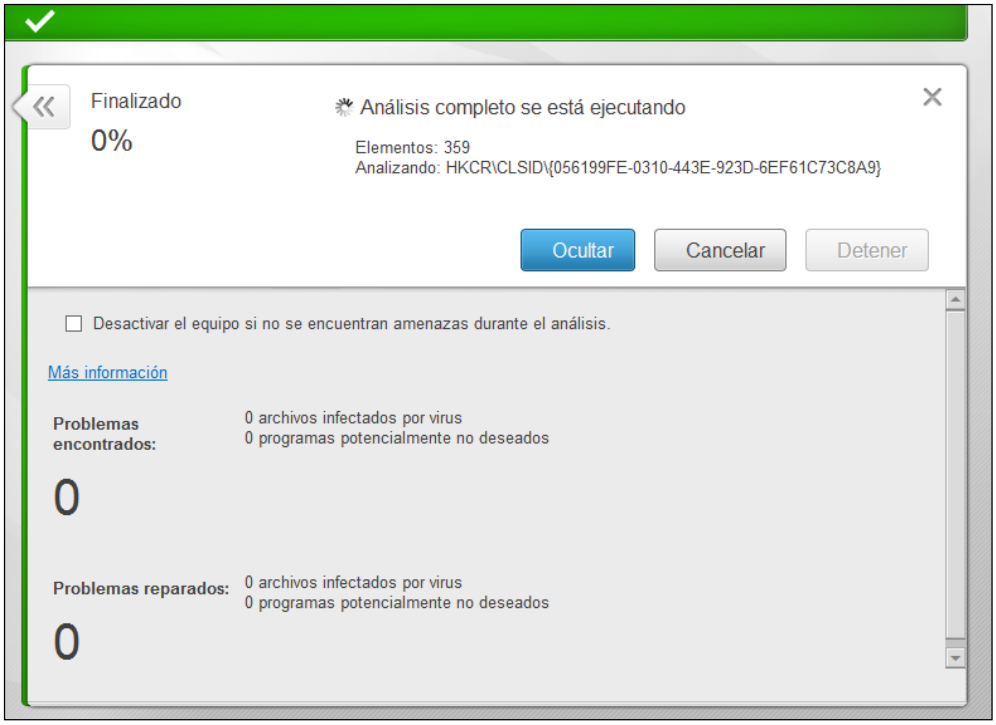




1.1.1.1.2 Análisis completo

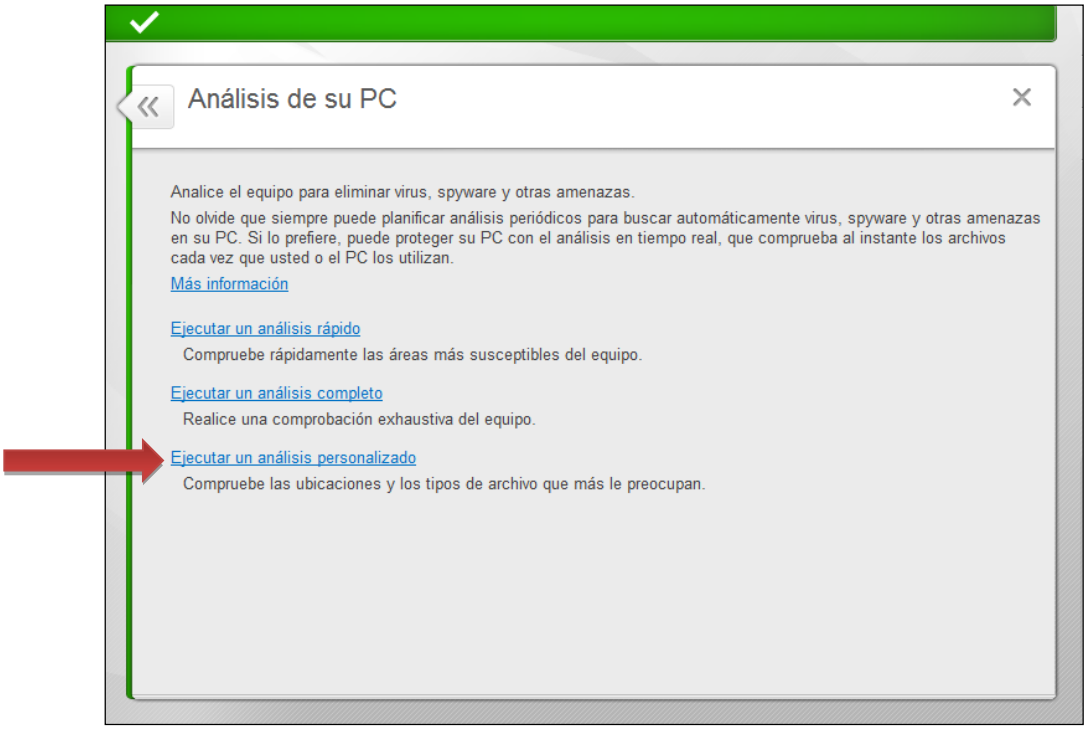
Este tipo de análisis permite verificar de forma minuciosa todas las áreas de su computador.

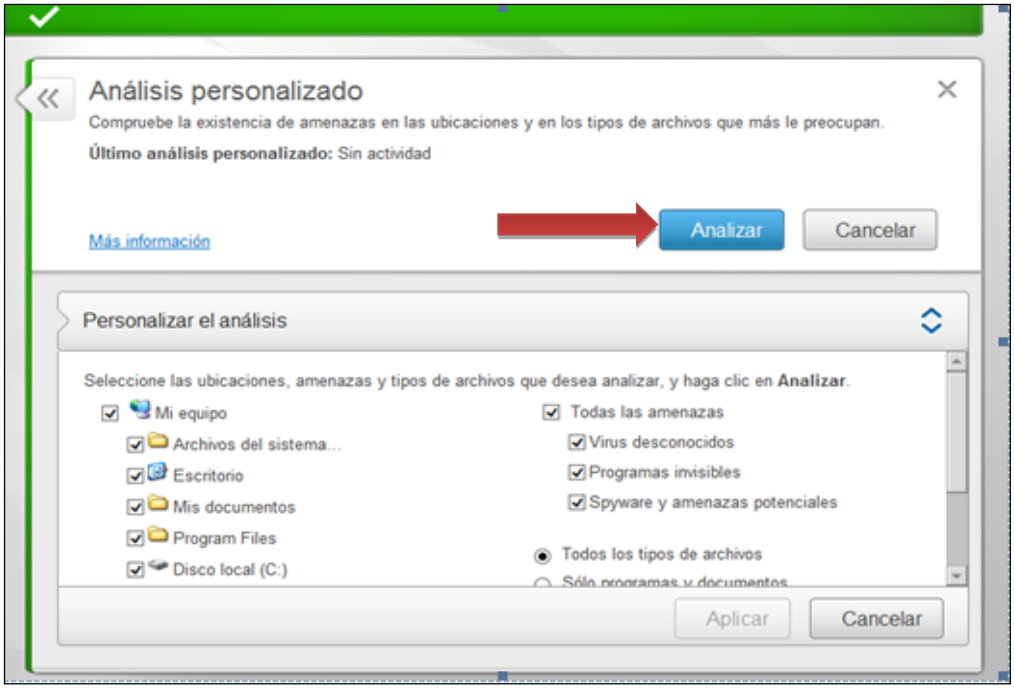




1.1.1.1.3 Análisis personalizado:

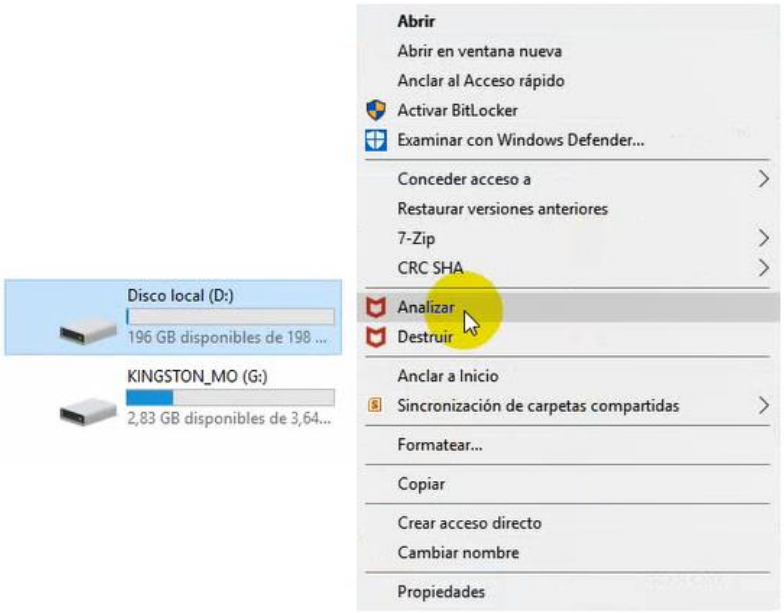
Este tipo de análisis permite escoger las áreas específicas que serán analizadas, junto con otras opciones:





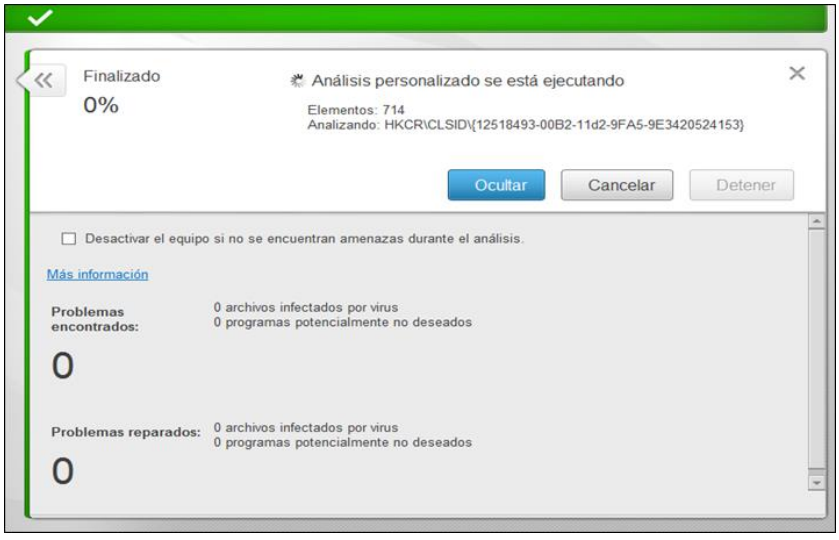
1.1.1.1.4 Análisis manual:

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

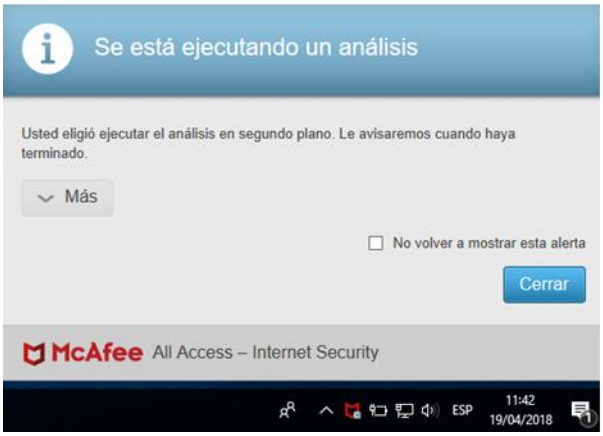


1.1.1.1.5 Visualización del progreso del análisis:

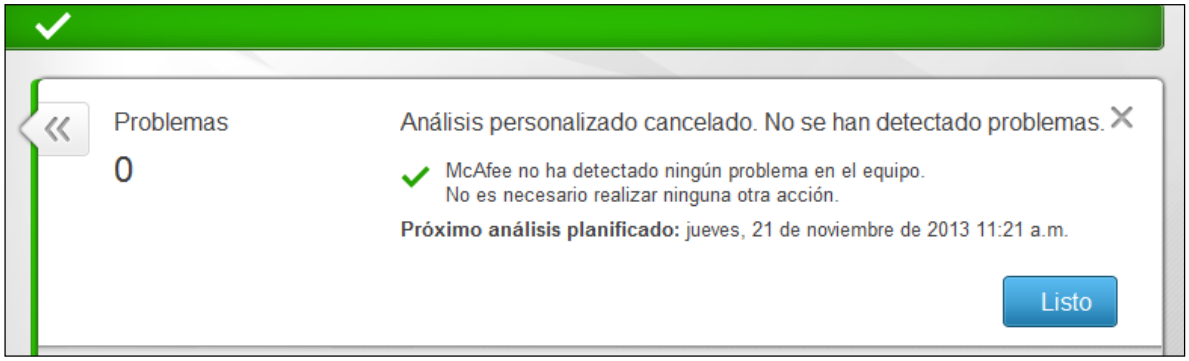
Cuando ejecuta un análisis, puede observar su progreso inmediatamente. McAfee muestra de forma simultánea los problemas que encuentra y los que repara. Entre estos problemas se encuentran archivos infectados por virus, programas potencialmente no deseados y cookies de rastreo. Si quedan problemas sin 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



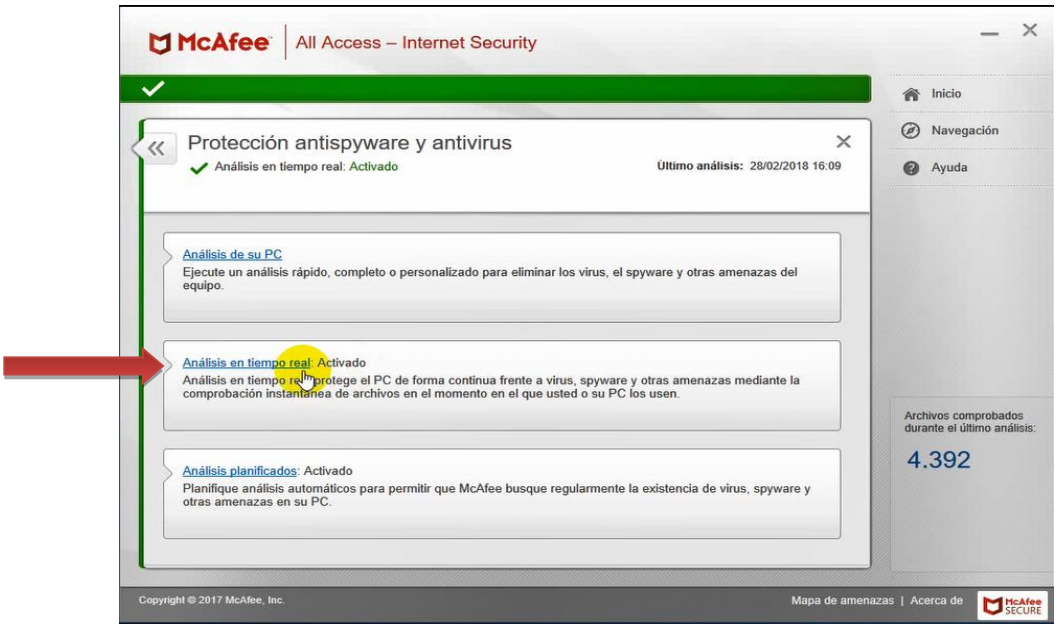
- *Detener:* Interrumpe el análisis para reanudarlo más tarde.
- *Reanudar:* Esta opción solo se activa cuando se detiene un análisis en progreso. Nos permite continuar con el análisis del computador.
- *Omitir:* Se pasa por alto un archivo que se está analizando actualmente, para pasar al siguiente 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:

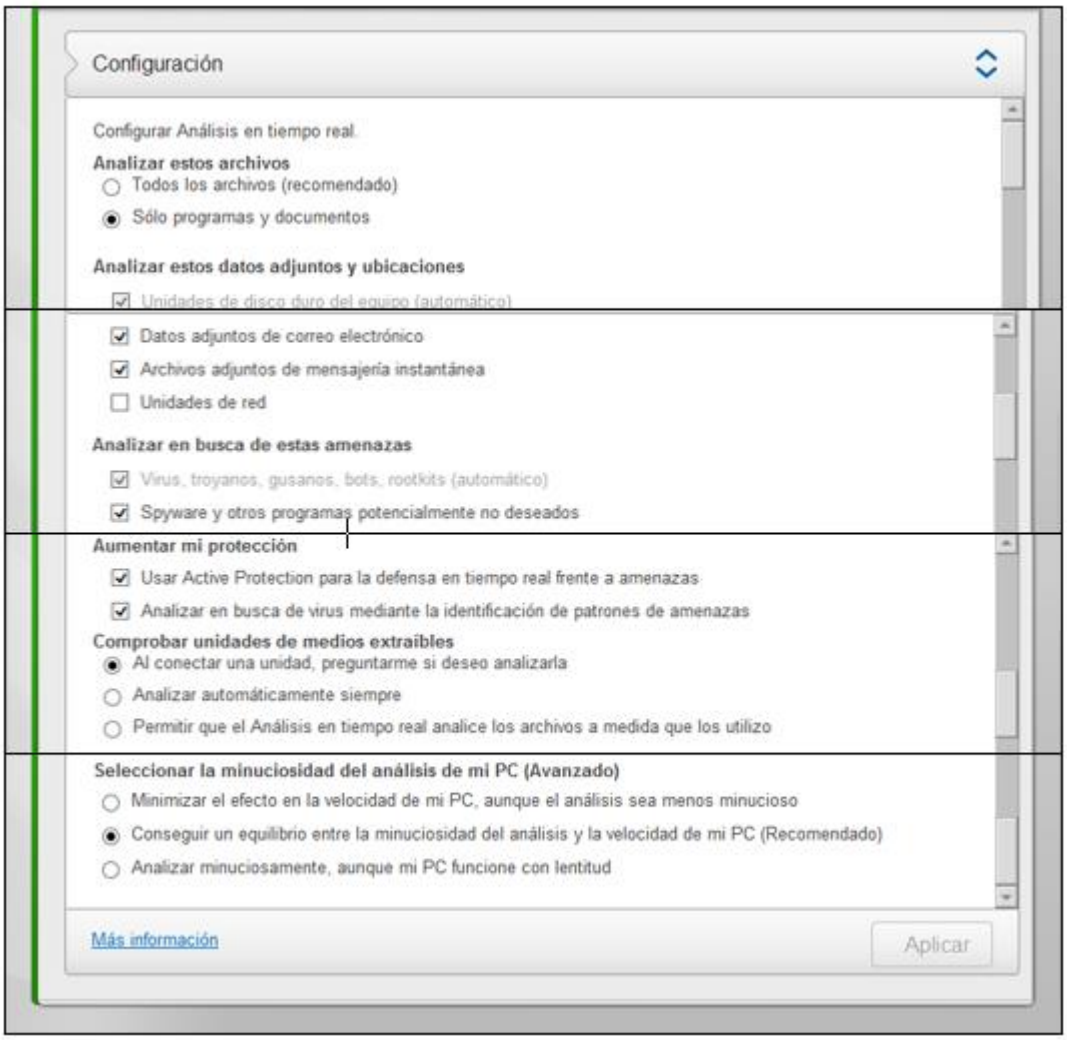
Los análisis en tiempo real comprueban los archivos en busca de virus cada vez que usted o el equipo acceden a ellos. Para acceder a su configuración, ingrese desde el Panel de inicio a *Protección de antispyware y antivirus,* luego *Análisis en tiempo real.*



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.

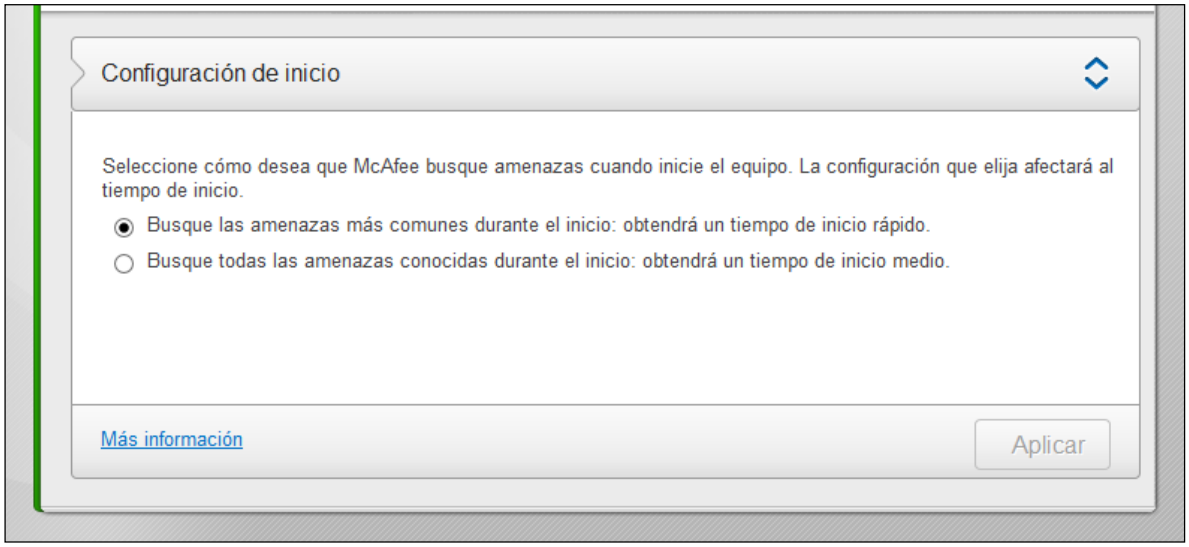
1.1.1.2.1 Configuración:

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



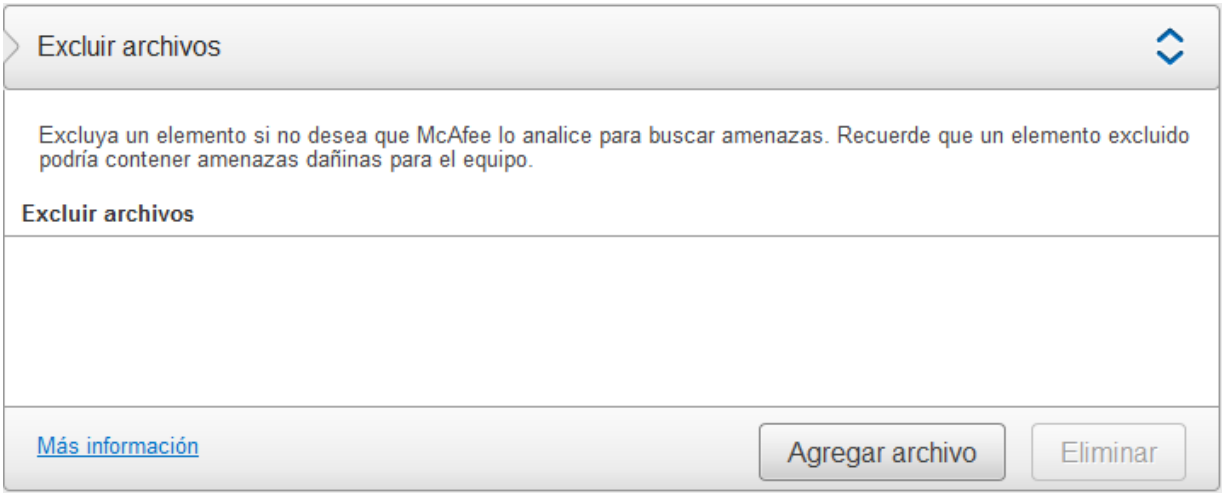
1.1.1.2.2 Configuración de Inicio:

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.

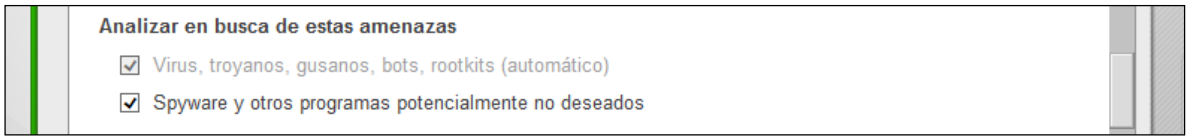
Archivos adjuntos y ubicaciones:

- *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

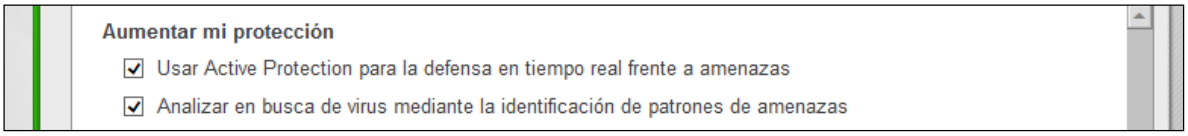
Cookies de rastreo. Detecta cookies de rastreo que controlan sus hábitos de navegación en la Web

- ***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)



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

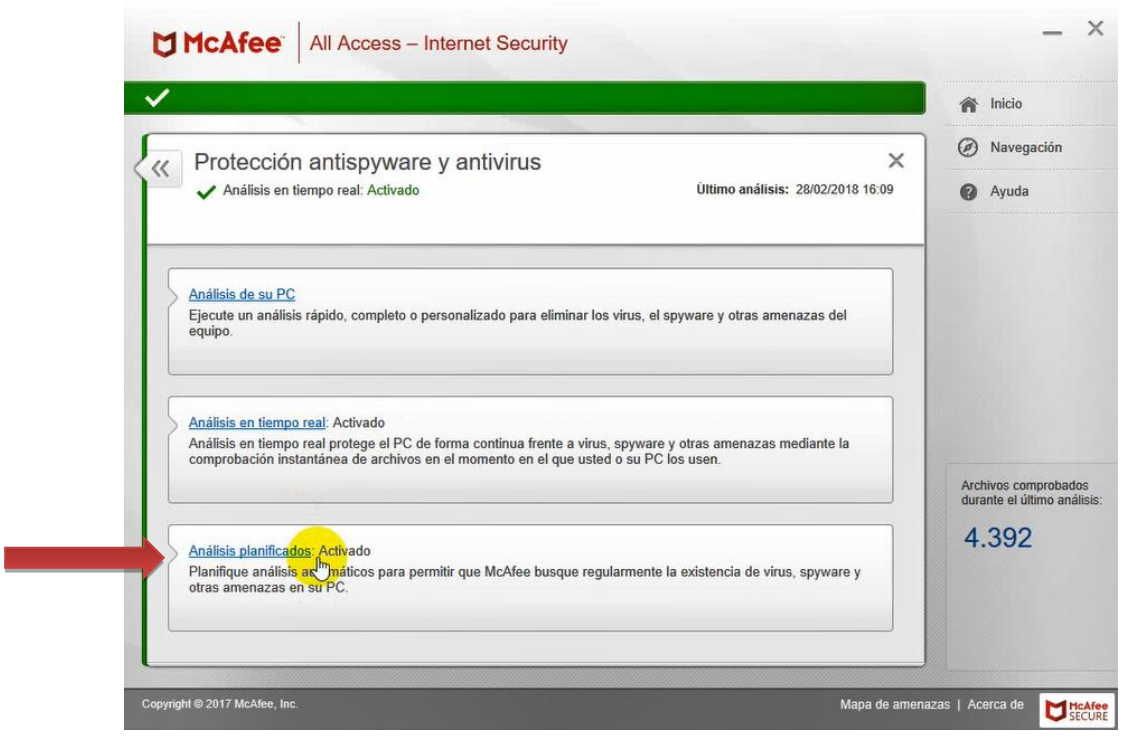


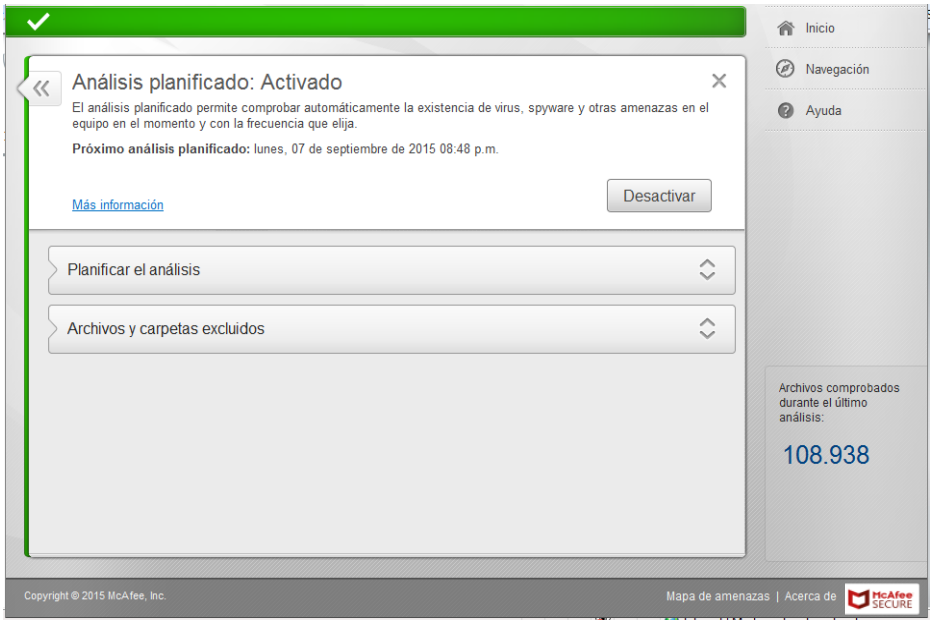
- **Analizar en busca de virus mediante la identificación de patrones de amenazas**. Permite la detección de amenazas que aunque no sean identificadas como tal, presentan comportamientos similares a amenazas ya identificadas. Finalmente para aplicar cualquier cambio realizado, marcamos *Aplicar.*

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

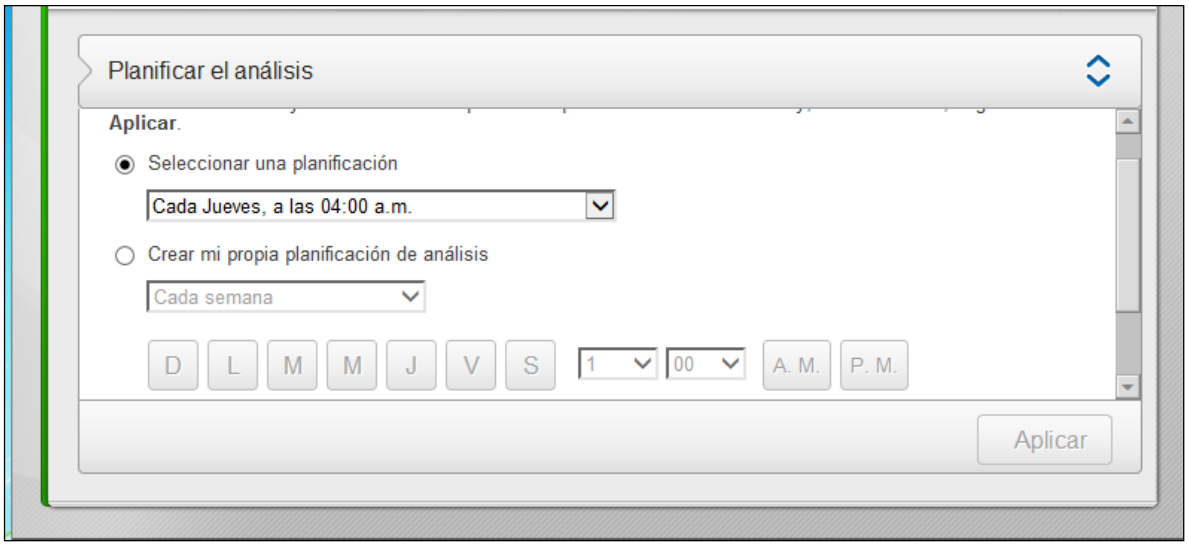
Los análisis planificados son uno de los elementos necesarios para asegurar la continua salud del equipo. Comprobado exhaustivamente (*Análisis completo*) el equipo en busca de virus y otras amenazas, de forma automática y periódicamente. Para acceder a la configuración desde el panel de inicio, ingrese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



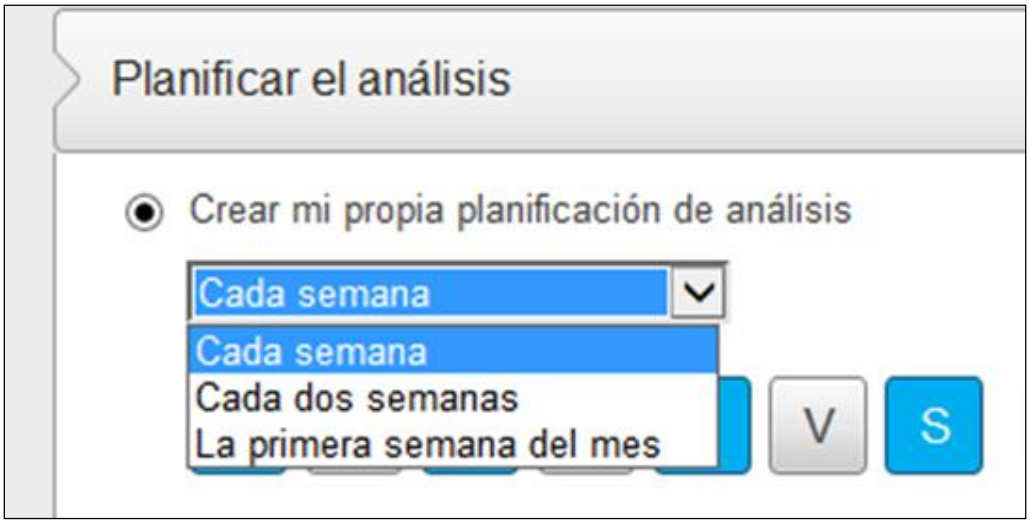


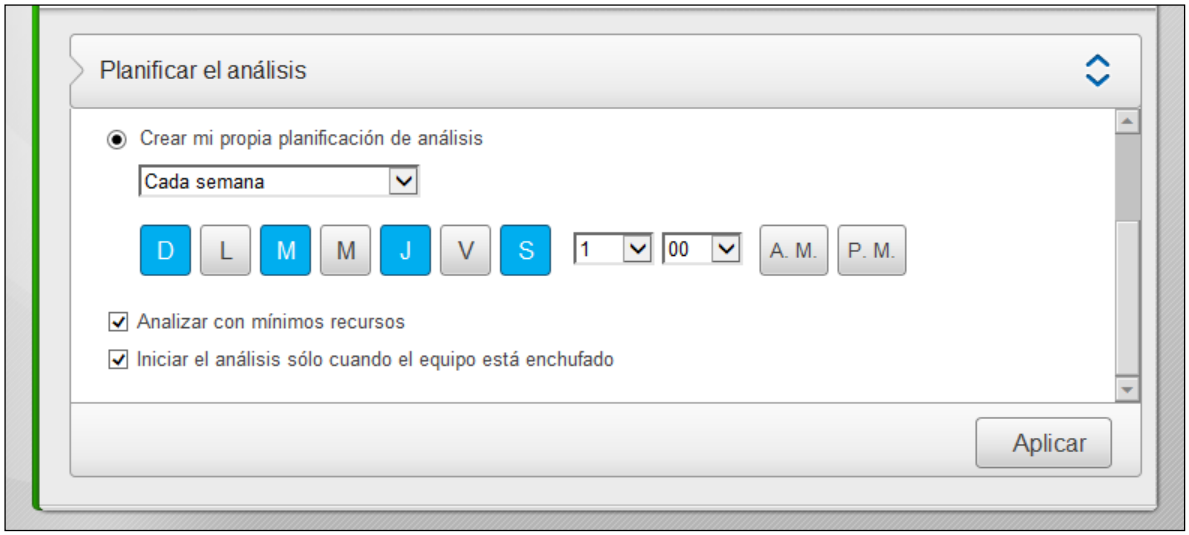
1.1.1.3.1 Planificación de análisis personalizado:

Planificación de análisis predeterminada



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.





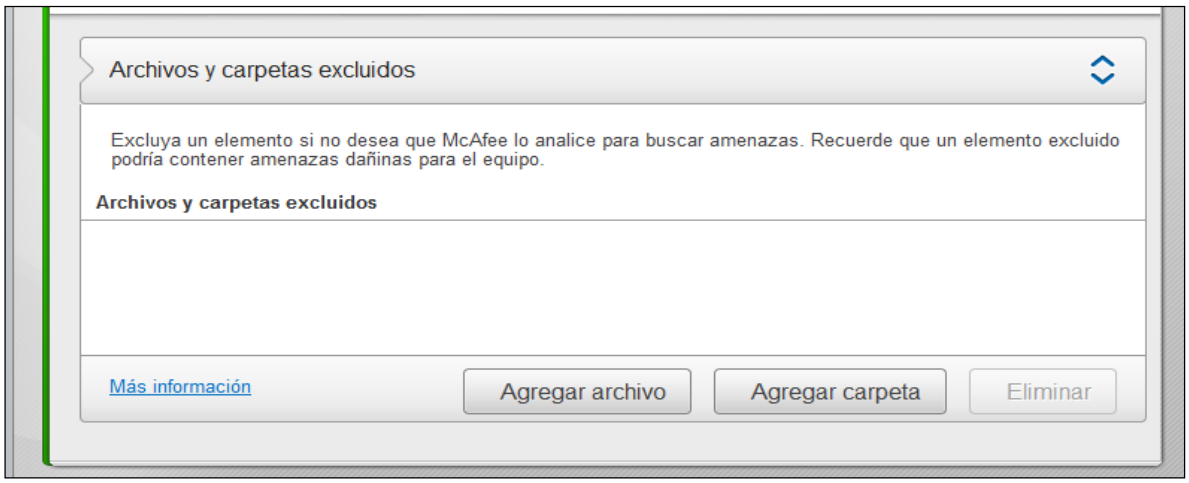
La planificación del análisis también puede modificarse según sus necesidades. Podemos seleccionar si el análisis se hará semanalmente, cada dos semanas o la primera semana de cada mes. Adicionalmente podemos escoger el día o los días y la hora en los cual se realizara el análisis.

Otras opciones

- La opción *Analizar con mínimos recursos* hace que el análisis utilice una mínima de la potencia de procesamiento del computador. AUnqué 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 archivo 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.

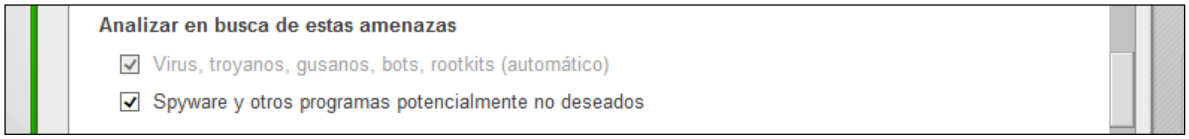
Archivos adjuntos y ubicaciones:

- *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

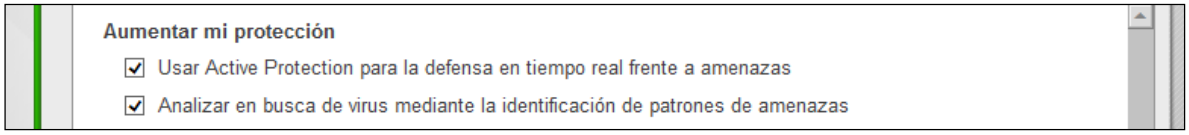
Cookies de rastreo. Detecta cookies de rastreo que controlan sus hábitos de navegación en la Web

- ***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)



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

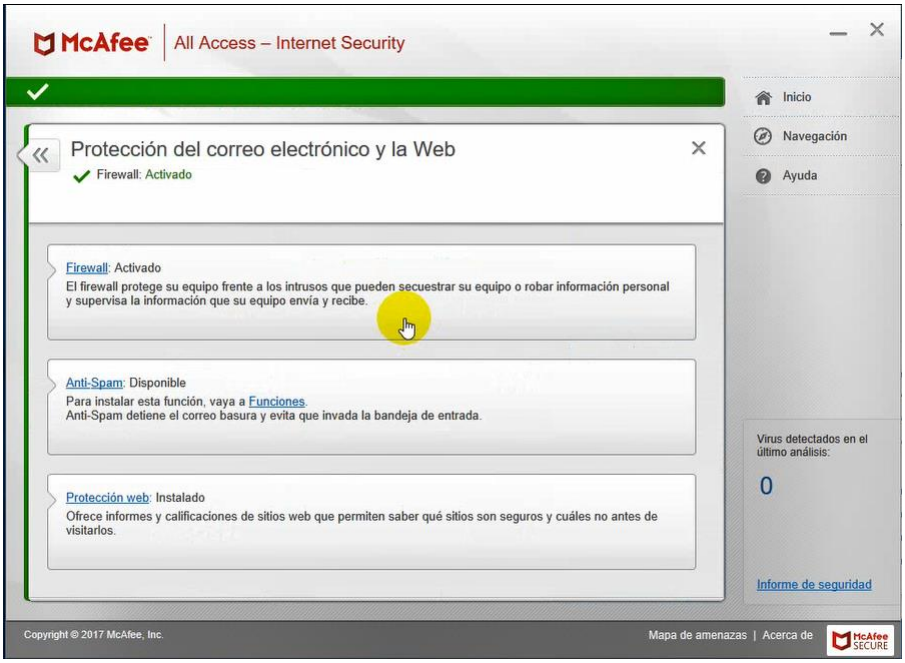


- **Analizar en busca de virus mediante la identificación de patrones de amenazas**. Permite la detección de amenazas que aunque no sean identificadas como tal, presentan comportamientos similares a amenazas ya identificadas. Finalmente para aplicar cualquier cambio realizado, marcamos *Aplicar.*

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

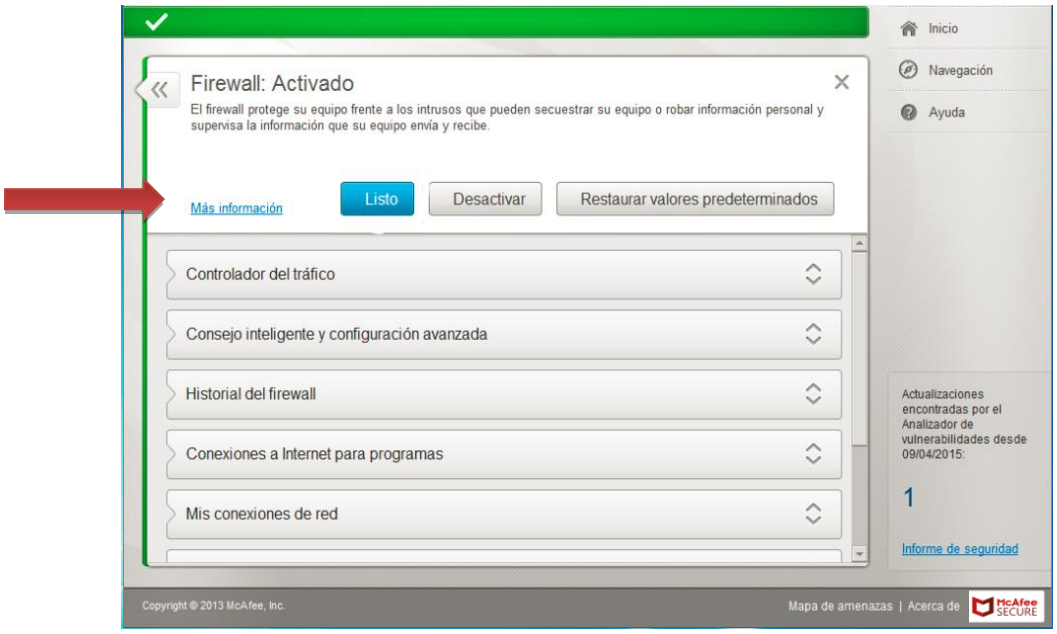
1.1.2 Protección del Correo Electrónico y la web:

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.



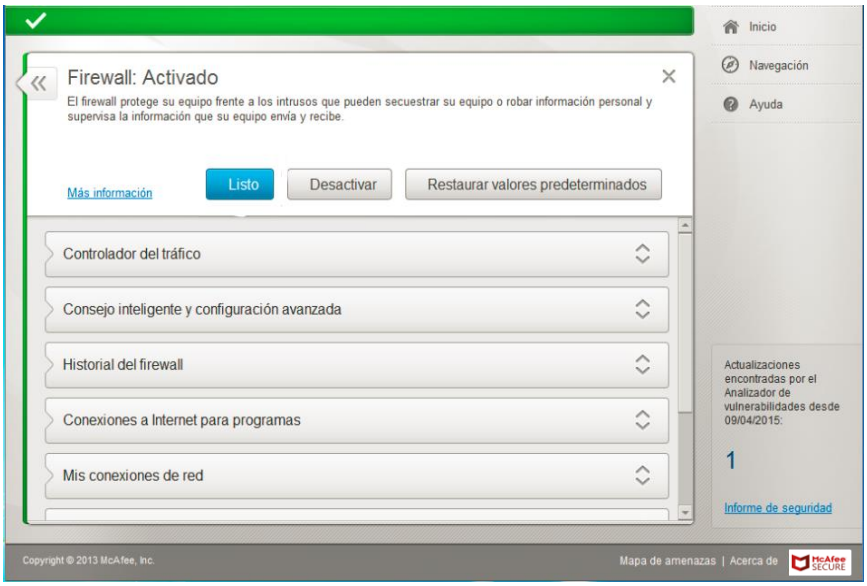
1.1.2.1 Firewall:

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.

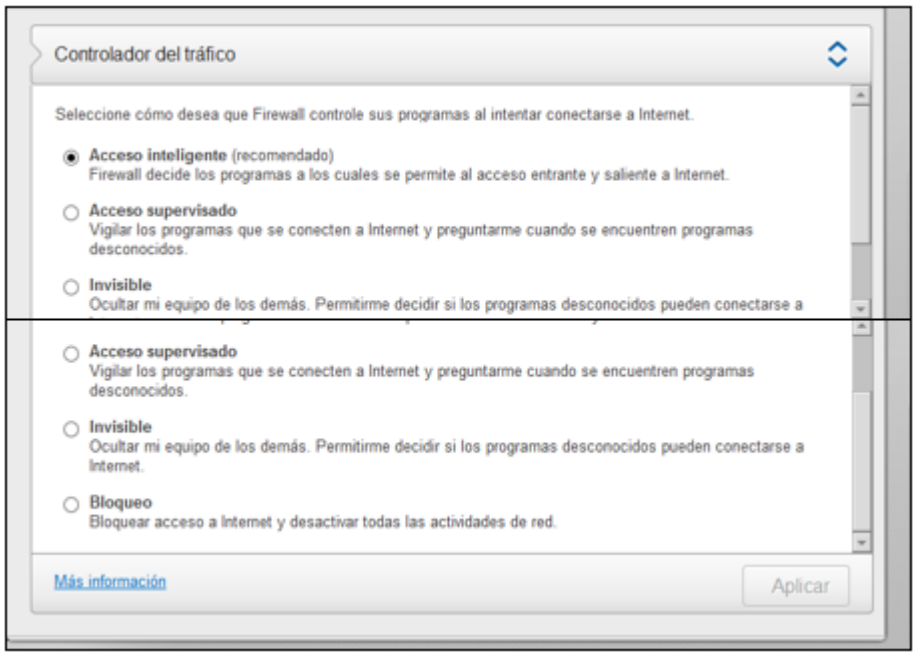


En la ventana de confirmación decida cuándo se reiniciara el firewall haciendo clic en la flecha situada junto a la opción *¿Cuándo desea que continúe el firewall*? El valor predeterminado es 15 minutos. Por último haga clic en *Desactivar.*

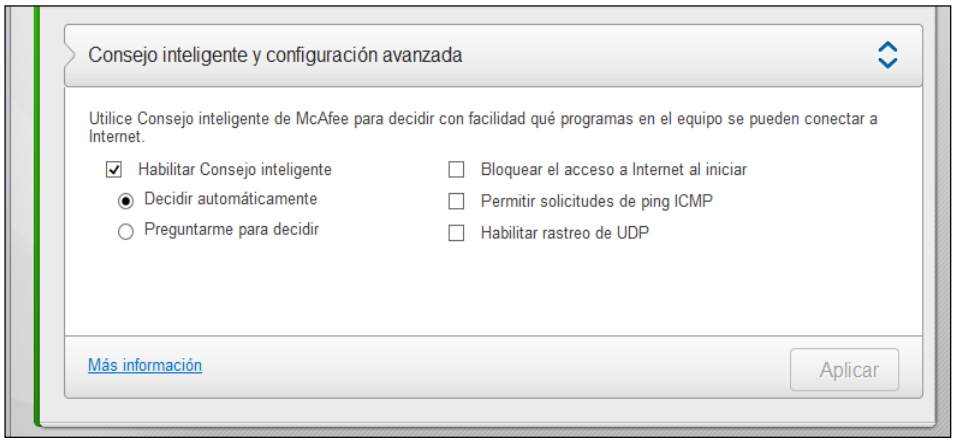
La desactivación de **Firewall** deja al equipo expuesto a las amenazas y el estado de la protección de la **Página de inicio** cambia e indica que el equipo está "en riesgo".

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

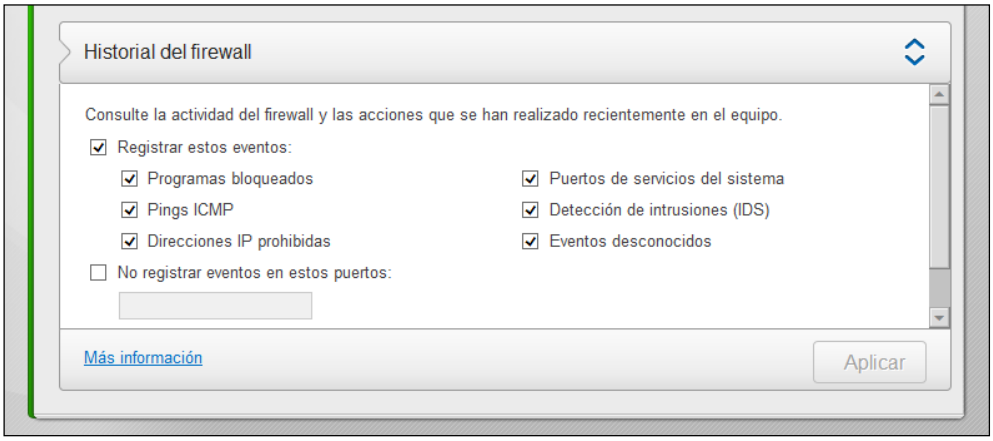
1.1.2.1.2 Controlador de Tráfico:



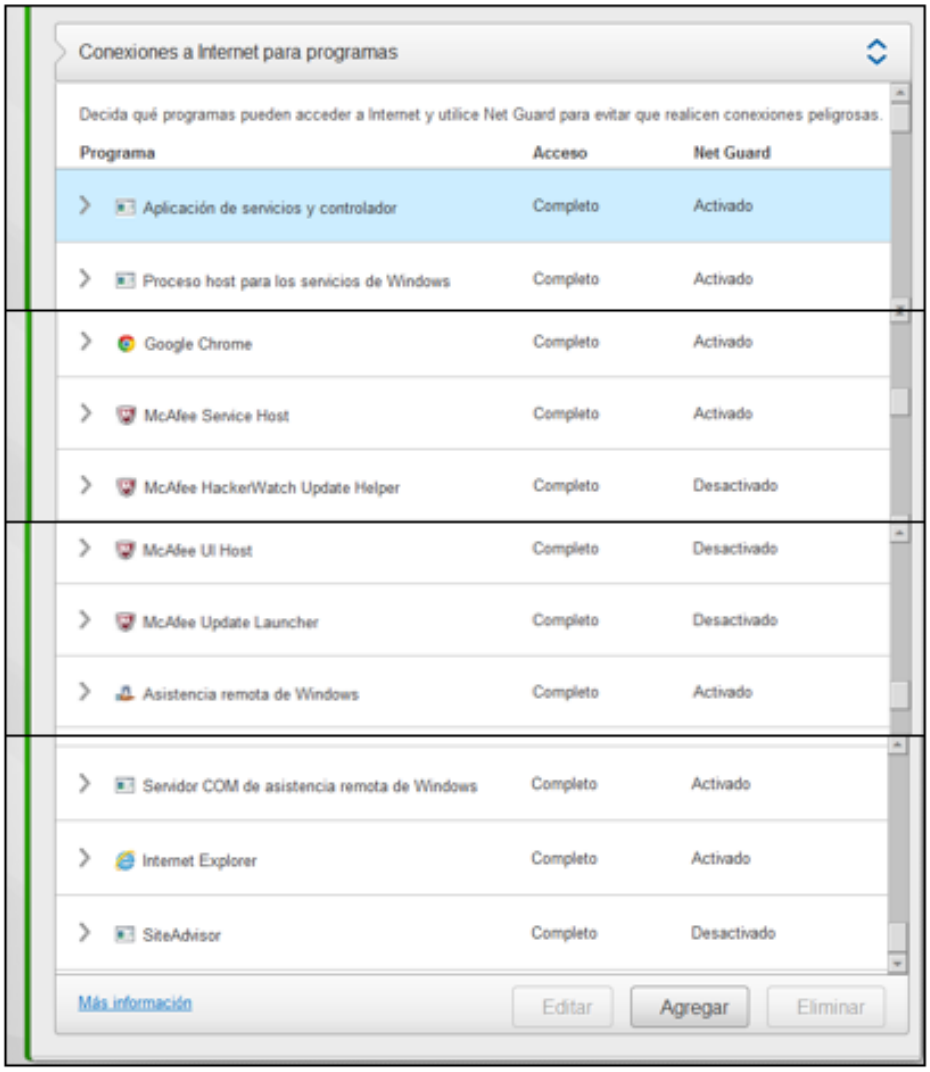
1.1.2.1.3 Consejo inteligente y configuración avanzada



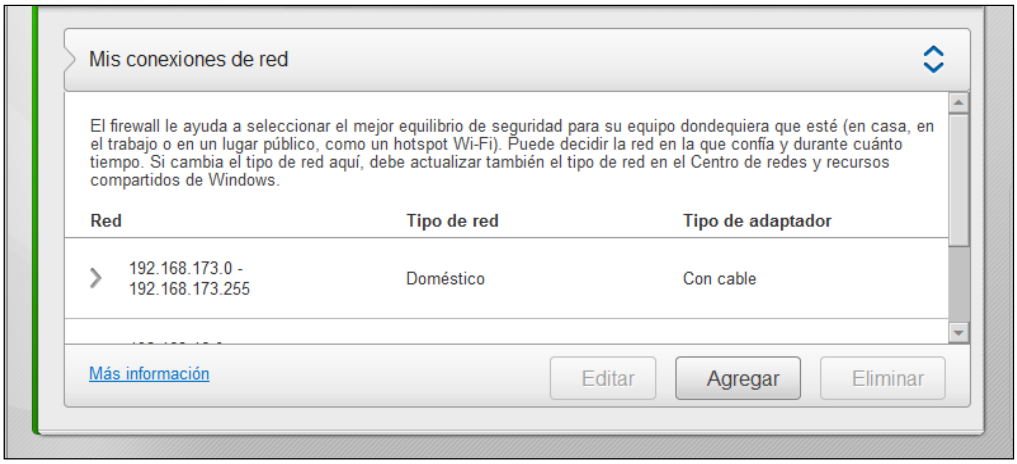
1.1.2.1.4 Historial de Firewall



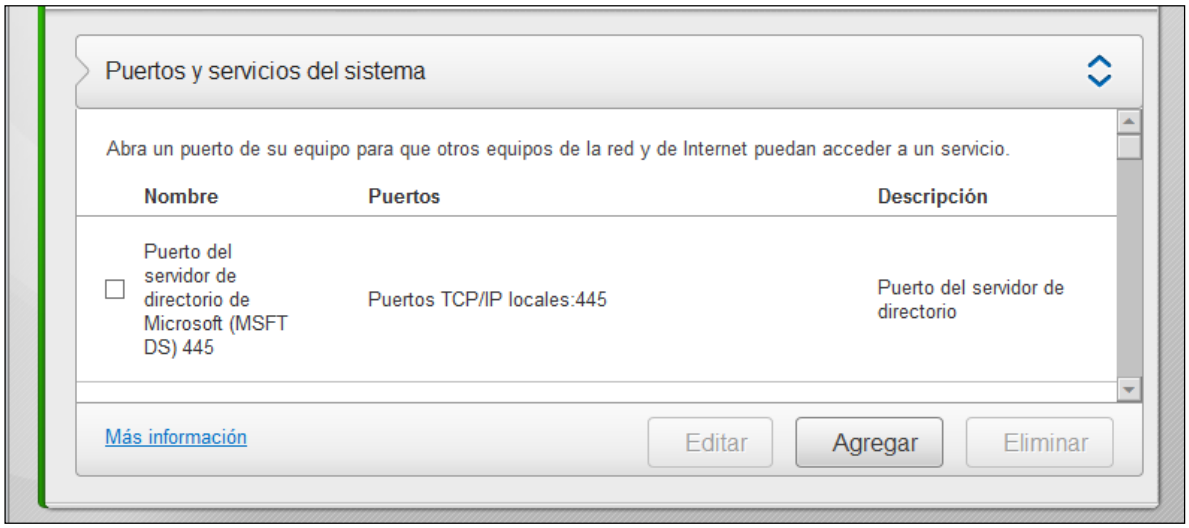
1.1.2.1.5 Conexiones a Internet para programas



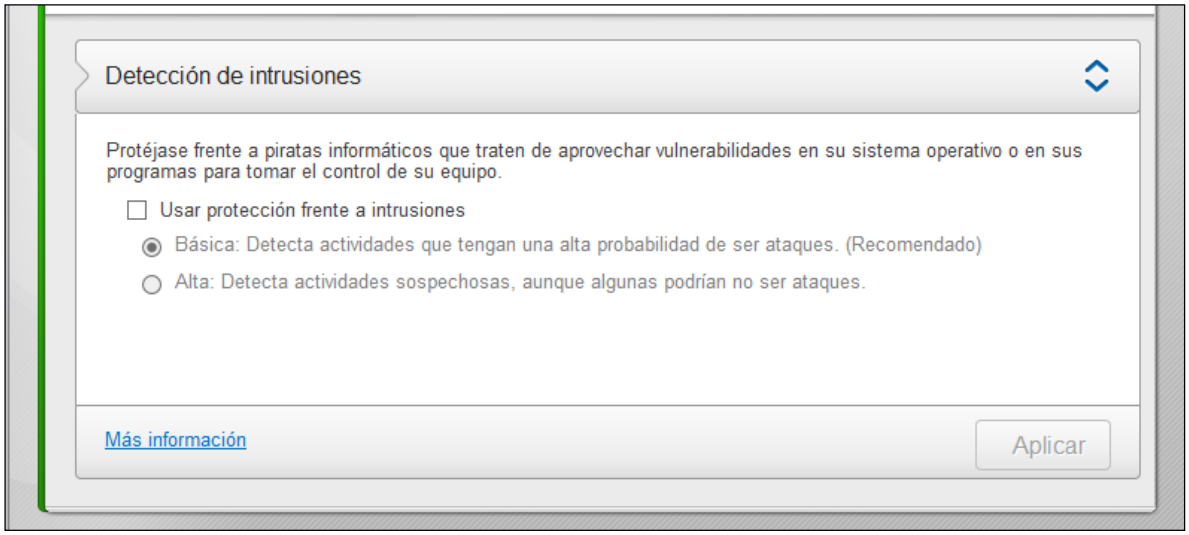
1.1.2.1.6 Mis Conexiones de Red



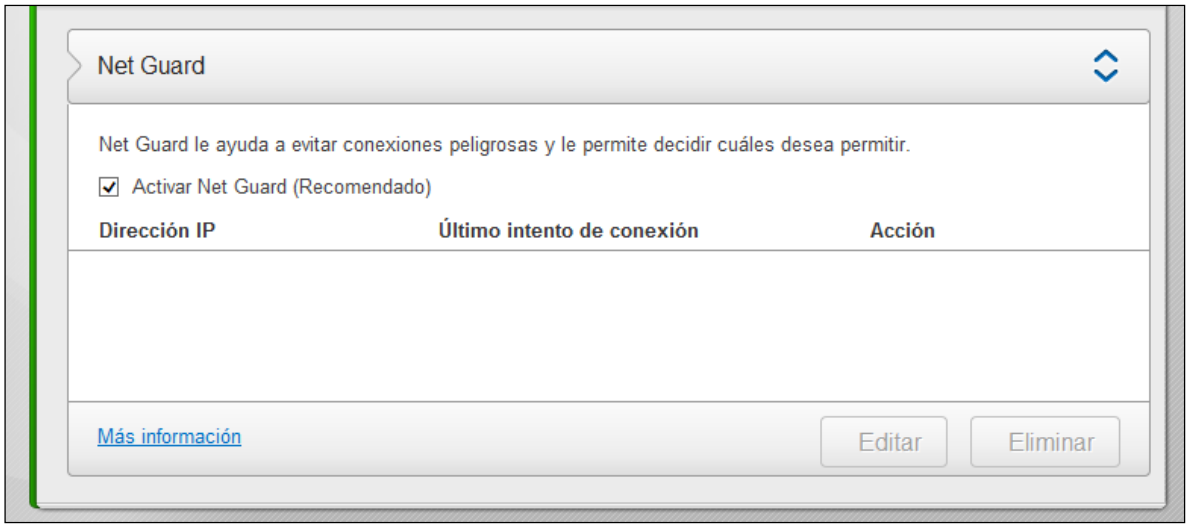
1.1.2.1.7 Puertos y Servicios del sistema



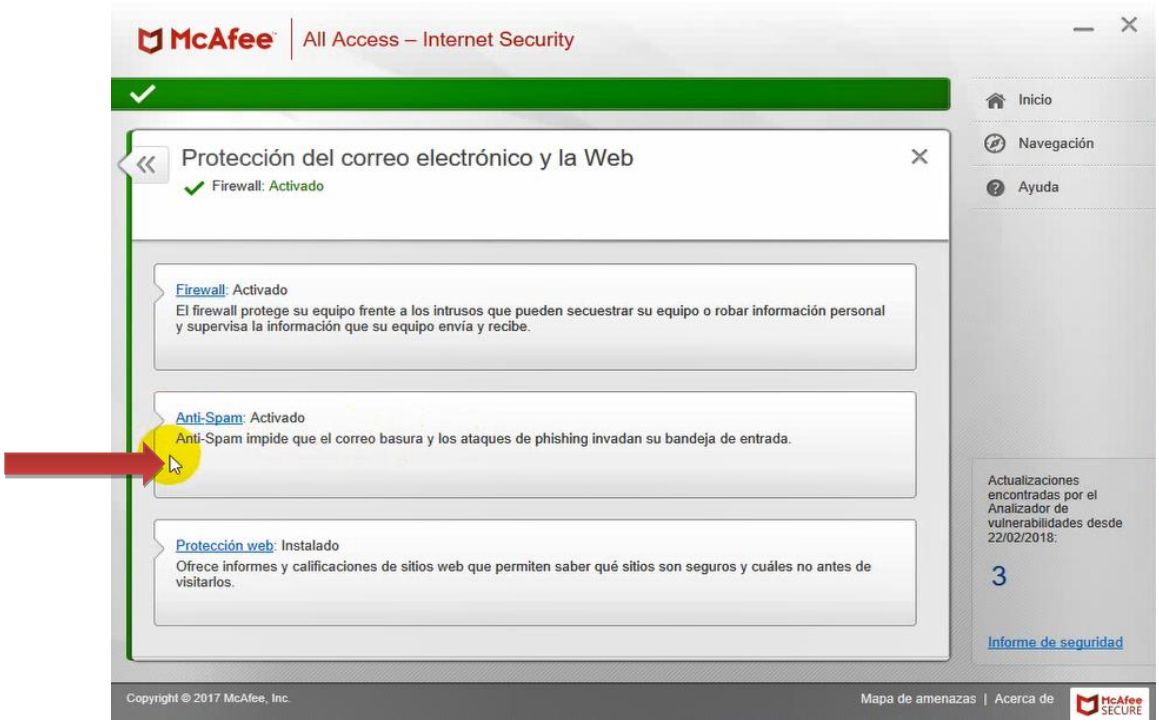
1.1.2.1.8 Detección de Intrusiones:

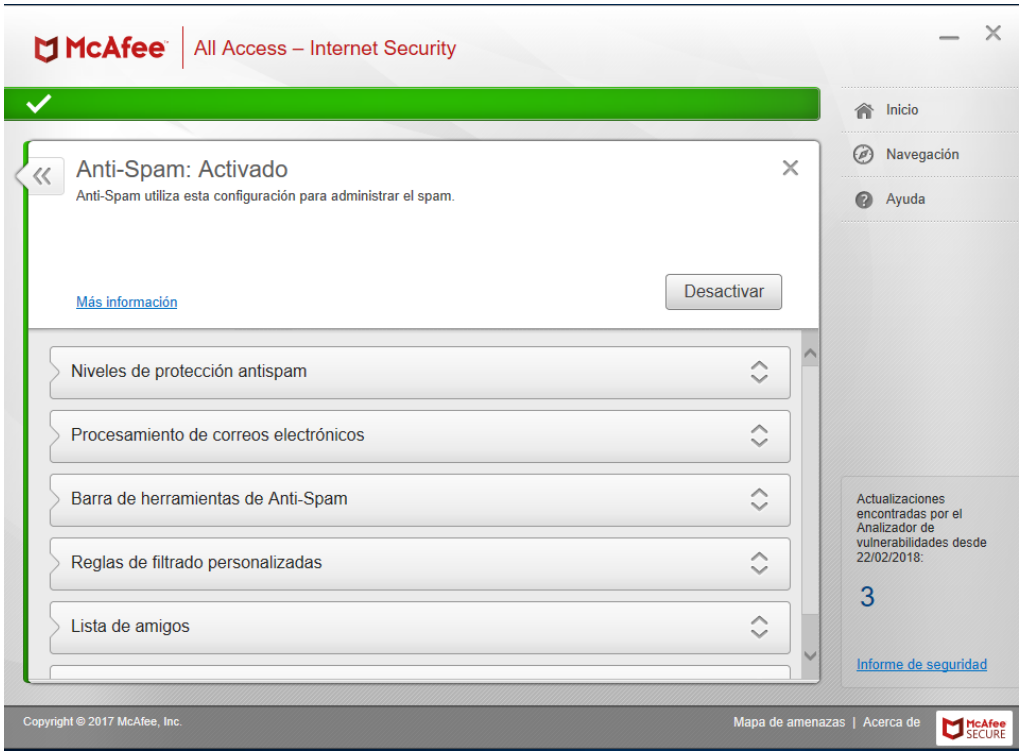


1.1.2.1.9 Net Guard:

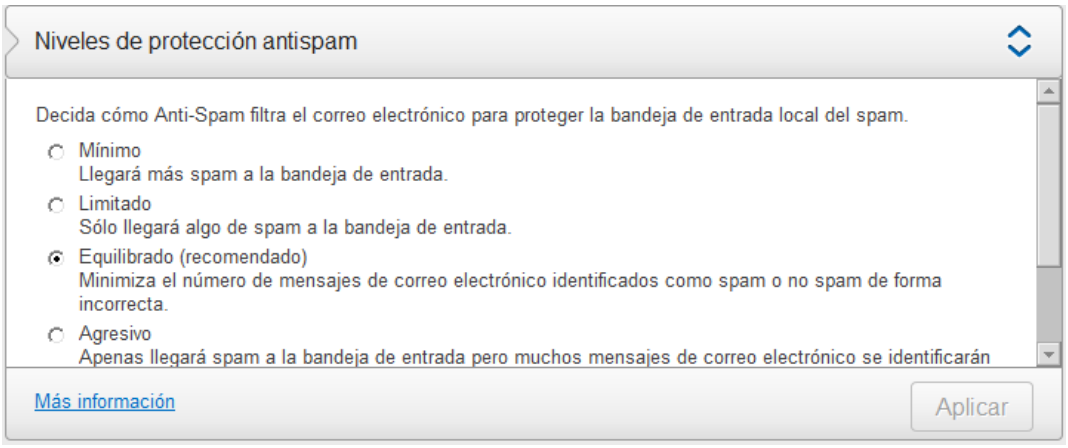


1.1.2.2 Anti-Spam:

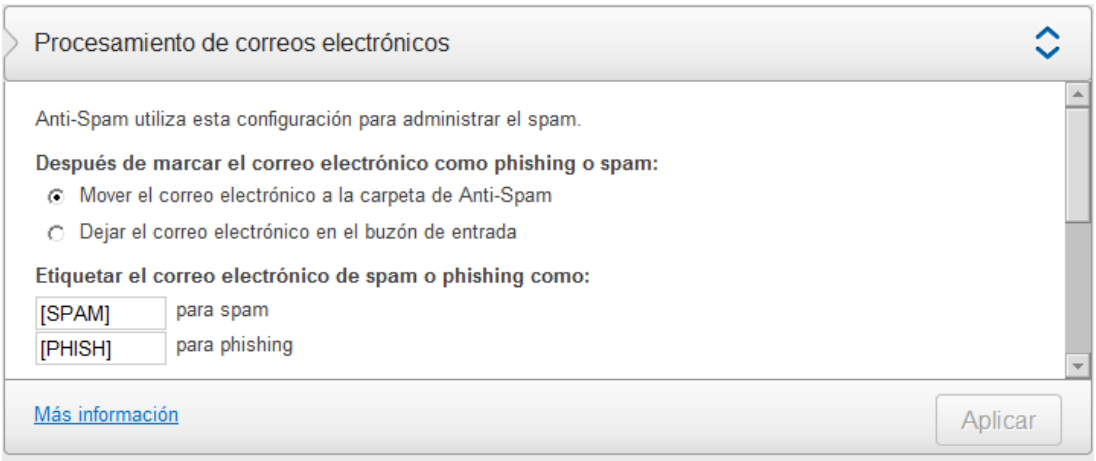




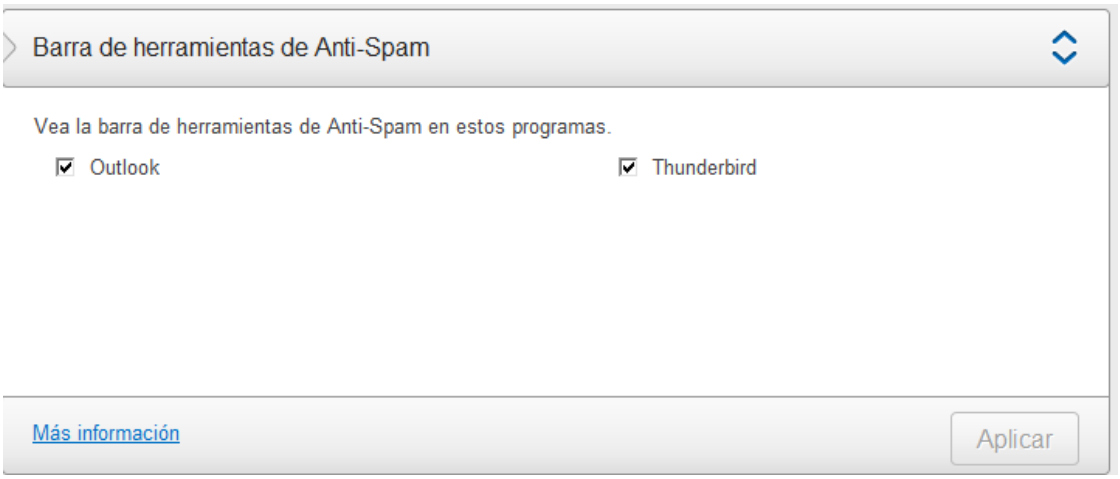
1.1.2.2.1 Niveles de protección Anti-Spam



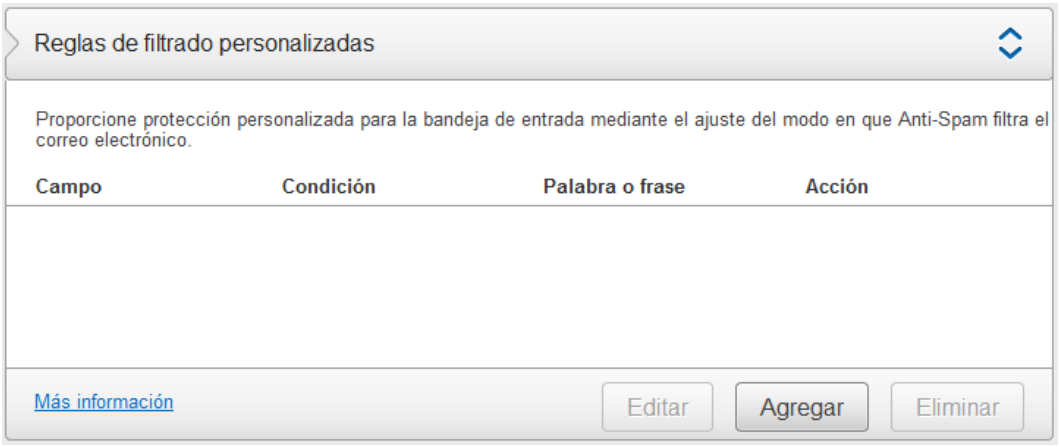
1.1.2.2.2 Procesamiento de correos electrónicos



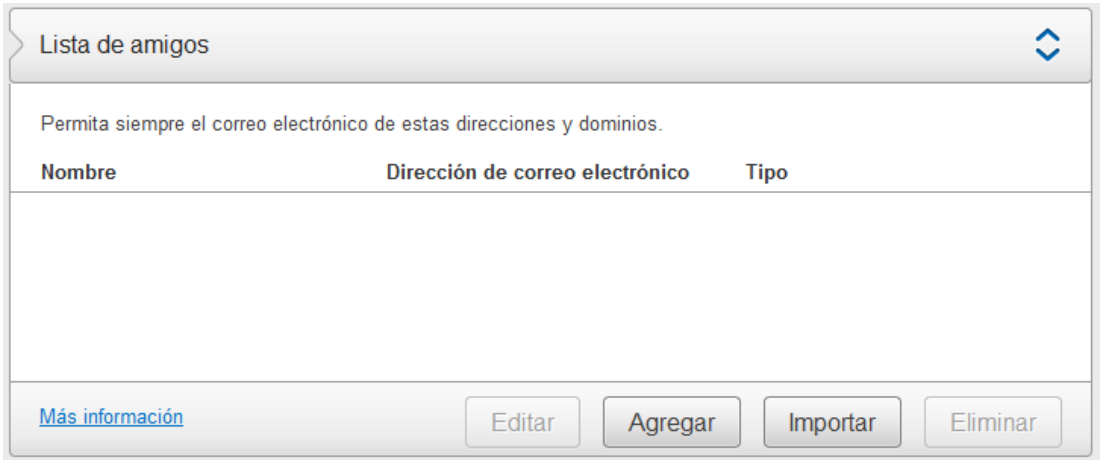
1.1.2.2.3 Barra de herramientas Anti-Spam



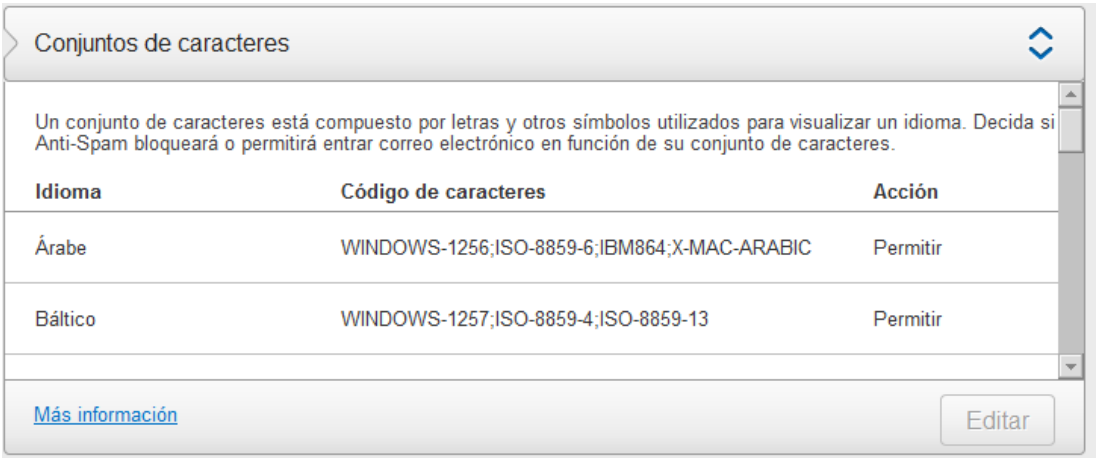
1.1.2.2.4 Reglas de filtrado personalizadas



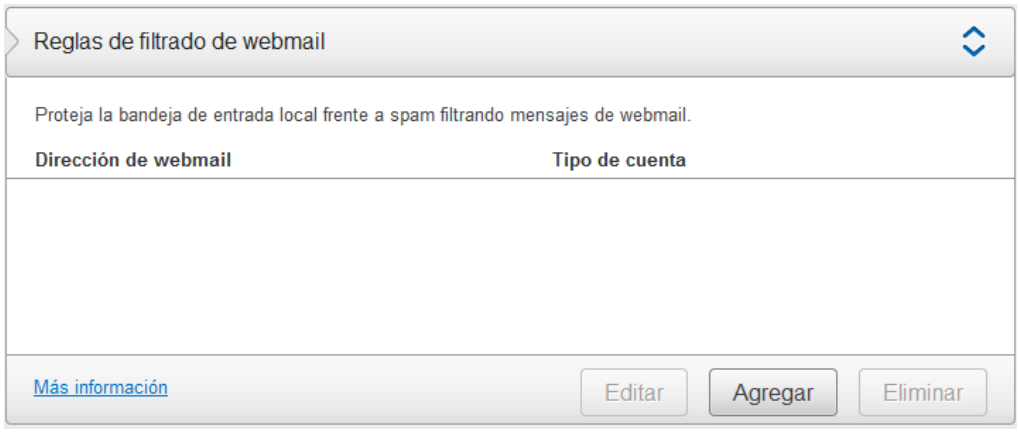
1.1.2.2.5 Lista de amigos



1.1.2.2.6 Conjunto de caracteres



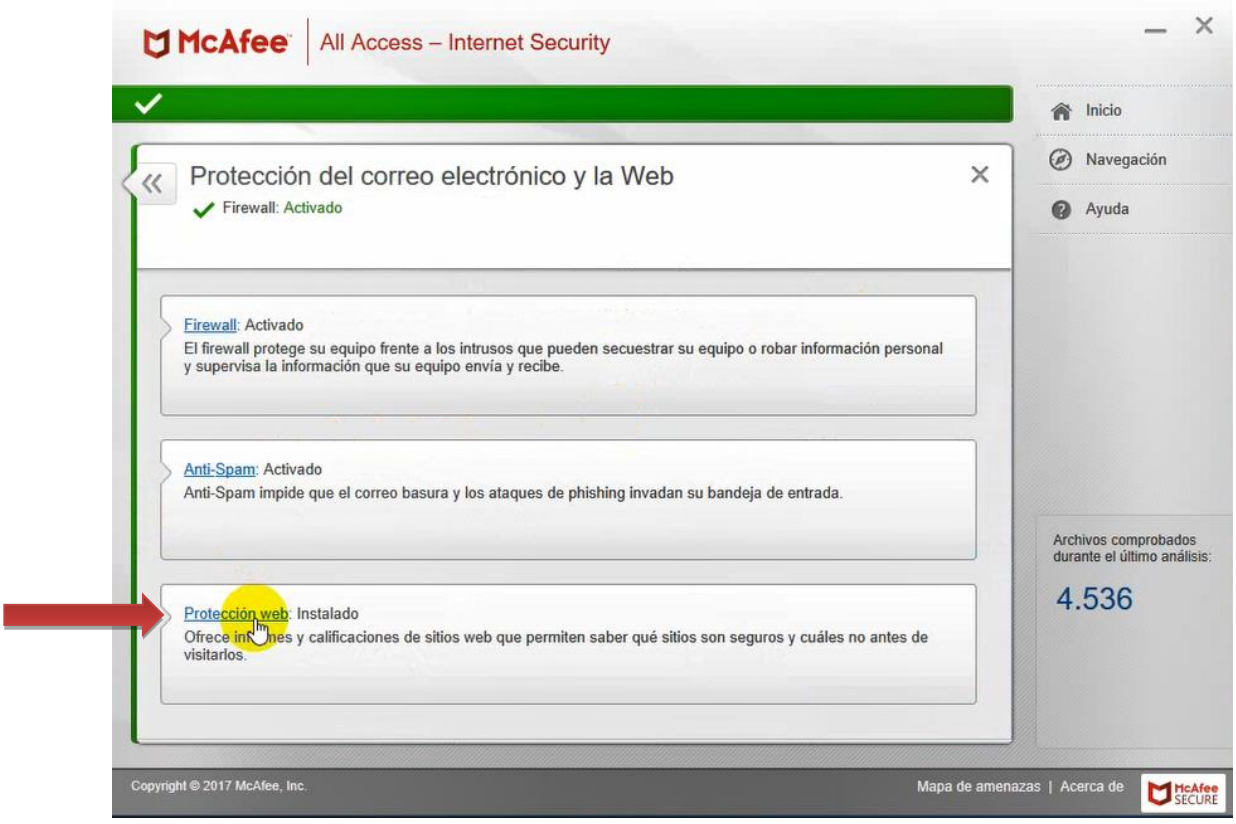
1.1.2.2.7 Reglas de filtrado de Webmail



1.1.2.2.8 Webmail filtrado

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.

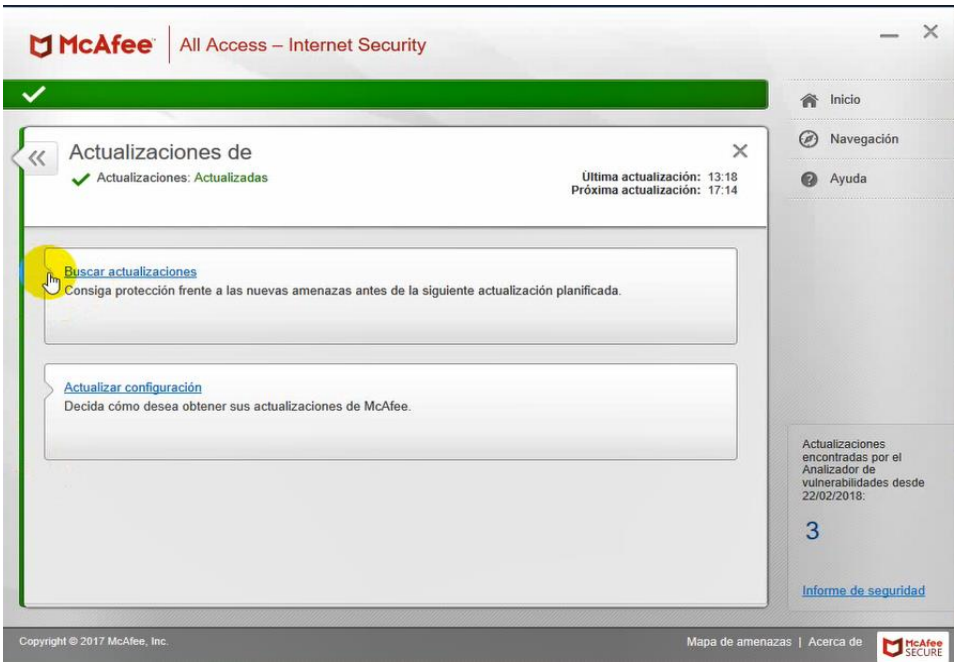

McAfee
Together is power.
SiteAdvisor®
› Soporte
› Acerca de McAfee
› Póngase en contacto con nosotros
› España - Español
Inicio
Seguridad Web
¿Cómo funciona?
Descargar
Recursos
Administradores del sitio Web
Inicio / ¿Cómo funciona?
¿Qué es el software SiteAdvisor?
El software SiteAdvisor es un galardonado 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.
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 cuado para bloquear los sitios peligrosos, evitar errores ortográficos y satisfacer todas las

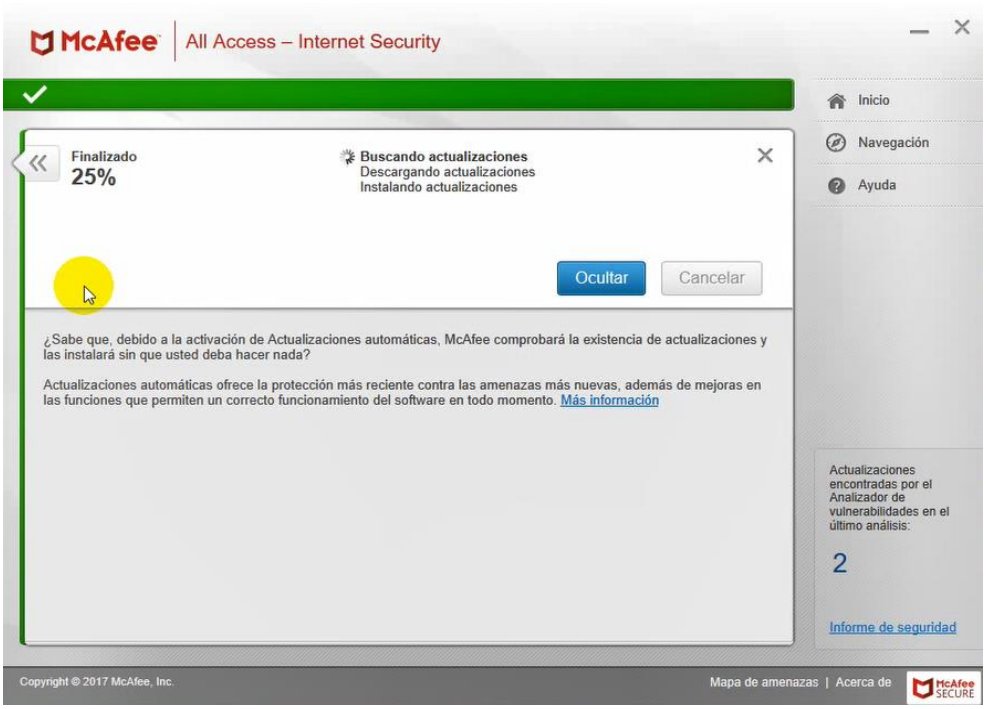
1.1.3 Actualizaciones de McAfee

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

1.1.3.1 Buscar actualizaciones

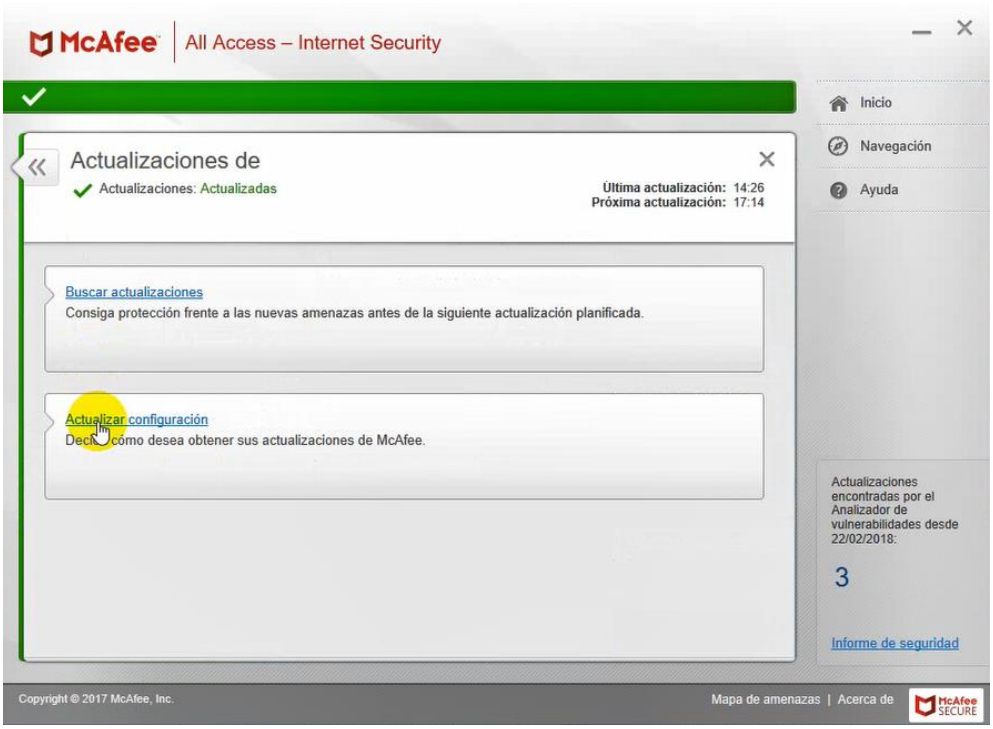
Consiga protección frente a nuevas amenazas antes de la siguiente actualización planificada.

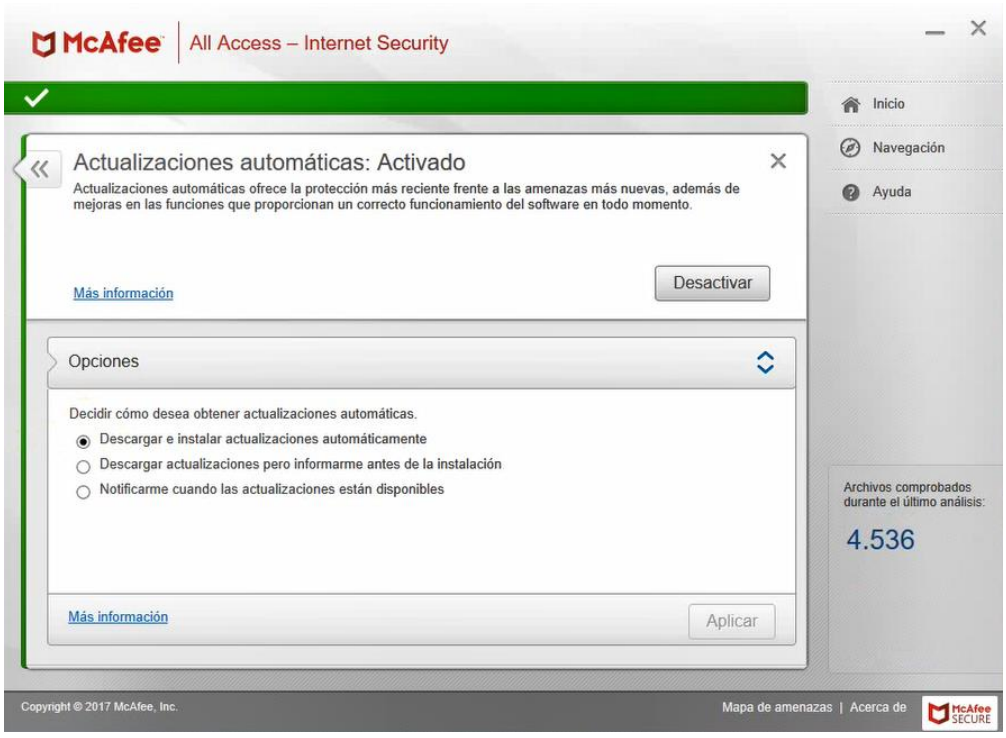




1.1.3.2 Actualizar configuración

Decida cómo desea obtener sus actualizaciones de McAfee

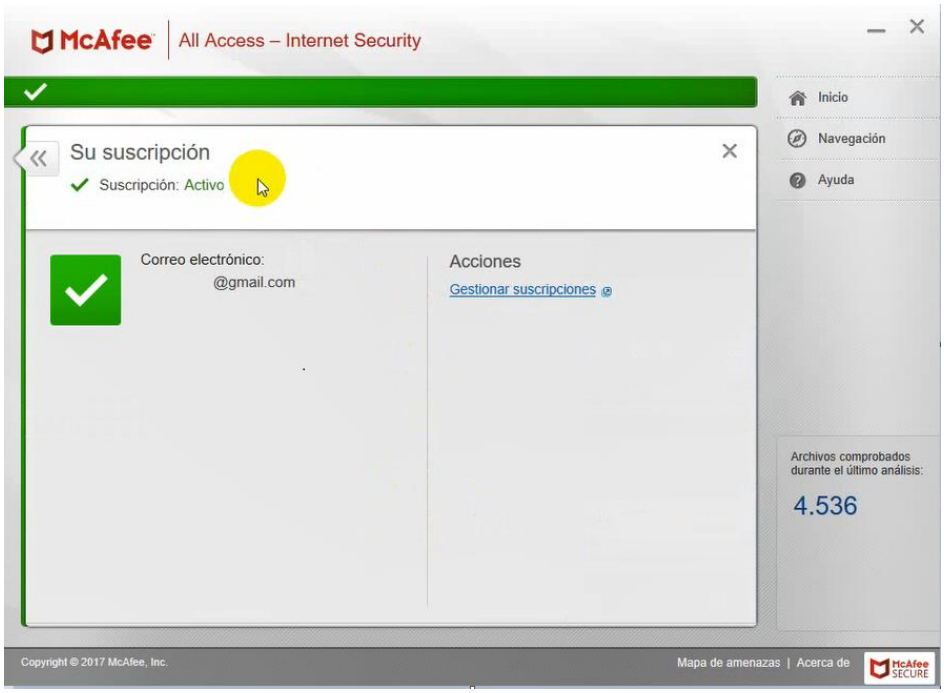




1.1.4 Su suscripción

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.

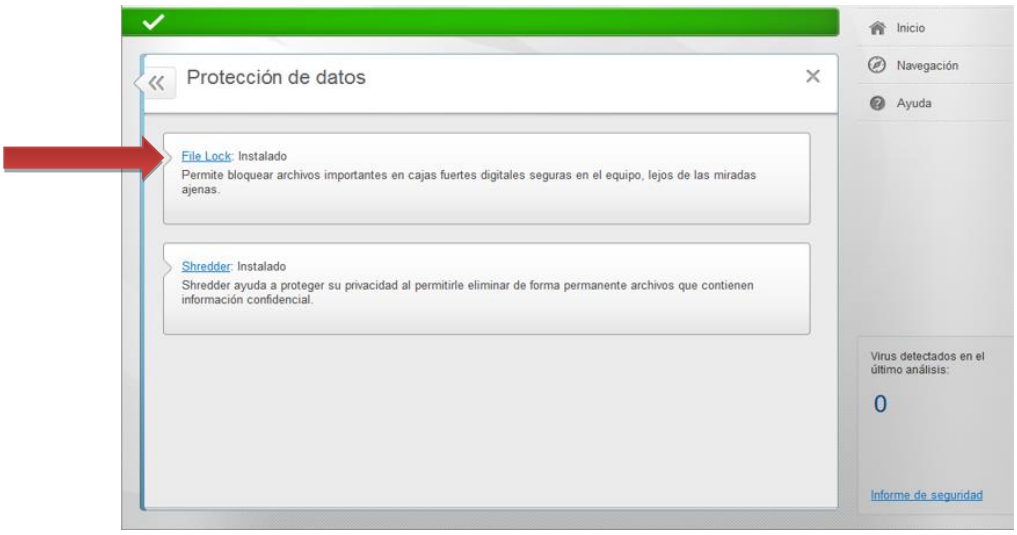


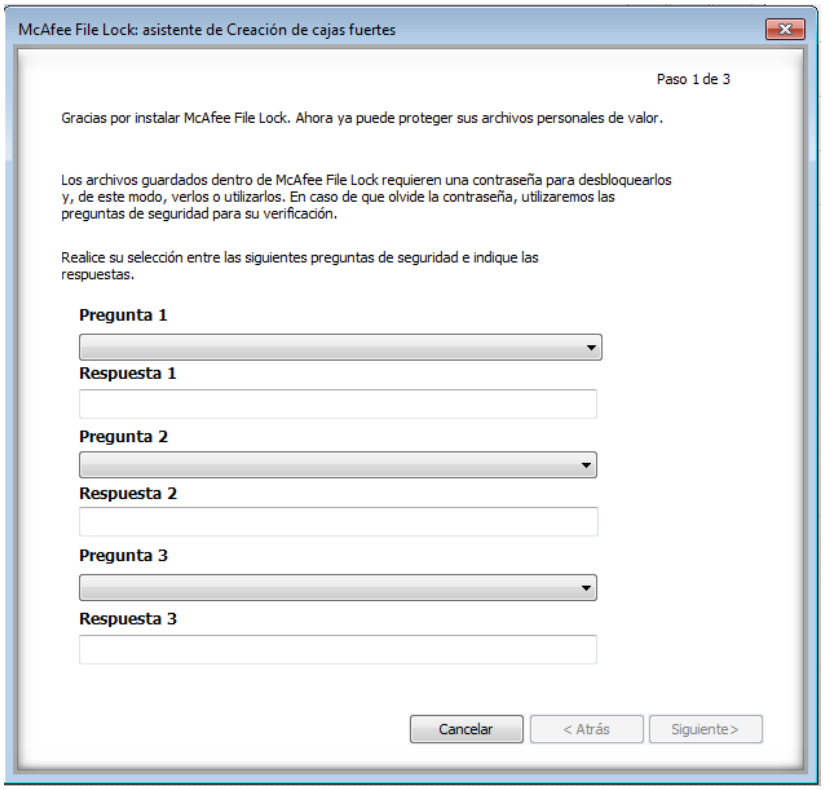
1.1.5 Protección de datos

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

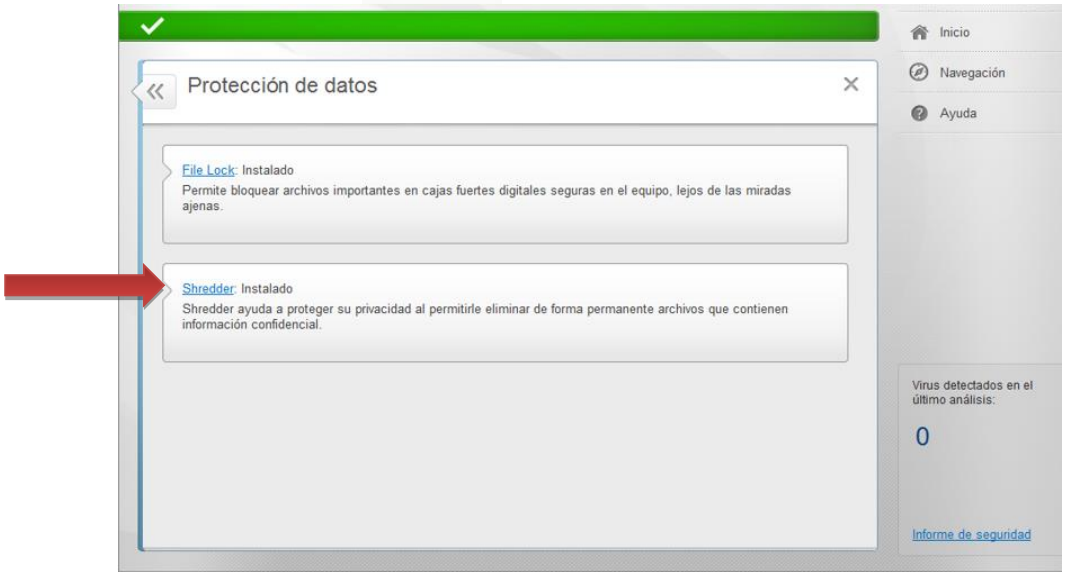
Permite bloquear archivos importantes en cajas fuertes digitales seguras en el equipo, lejos de las miradas ajenas.



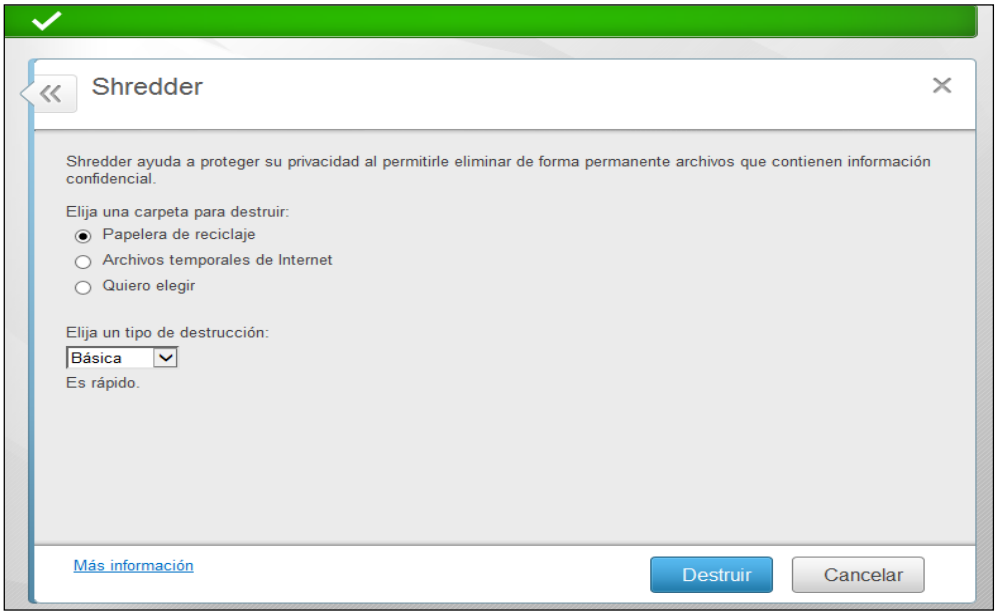


1.1.5.2 Shredder:

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

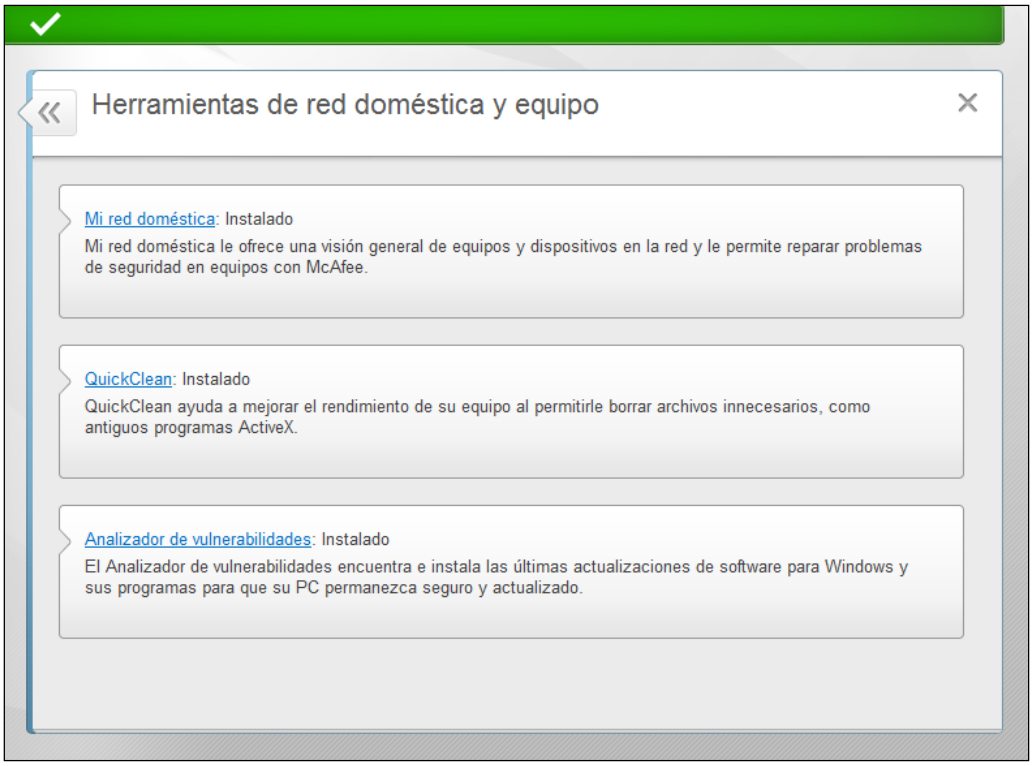


Puede elegir destruir los archivos de la Papelera de reciclaje, Archivos temporales, además de poder realizar una destrucción rápida, básica, segura, exhaustiva o completa.



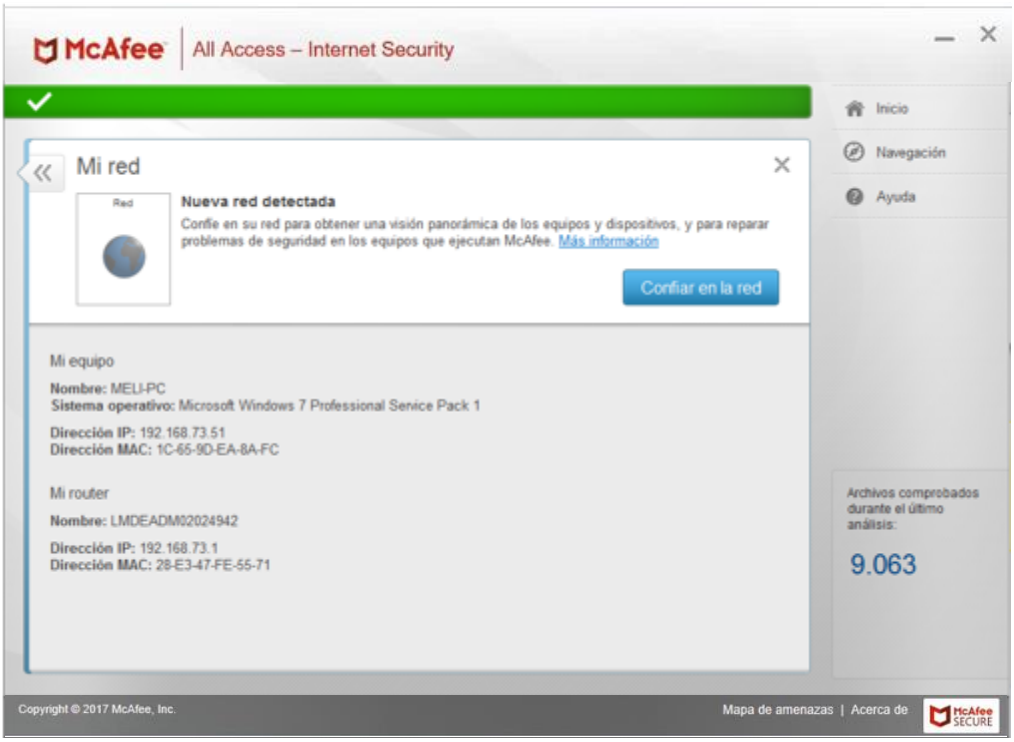
1.1.6 Herramientas de red doméstica y equipo

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.



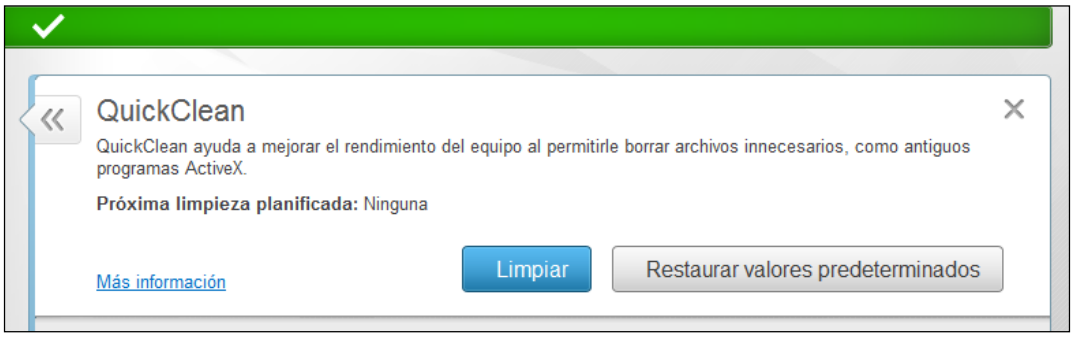
1.1.6.1 Mi red Doméstica:

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



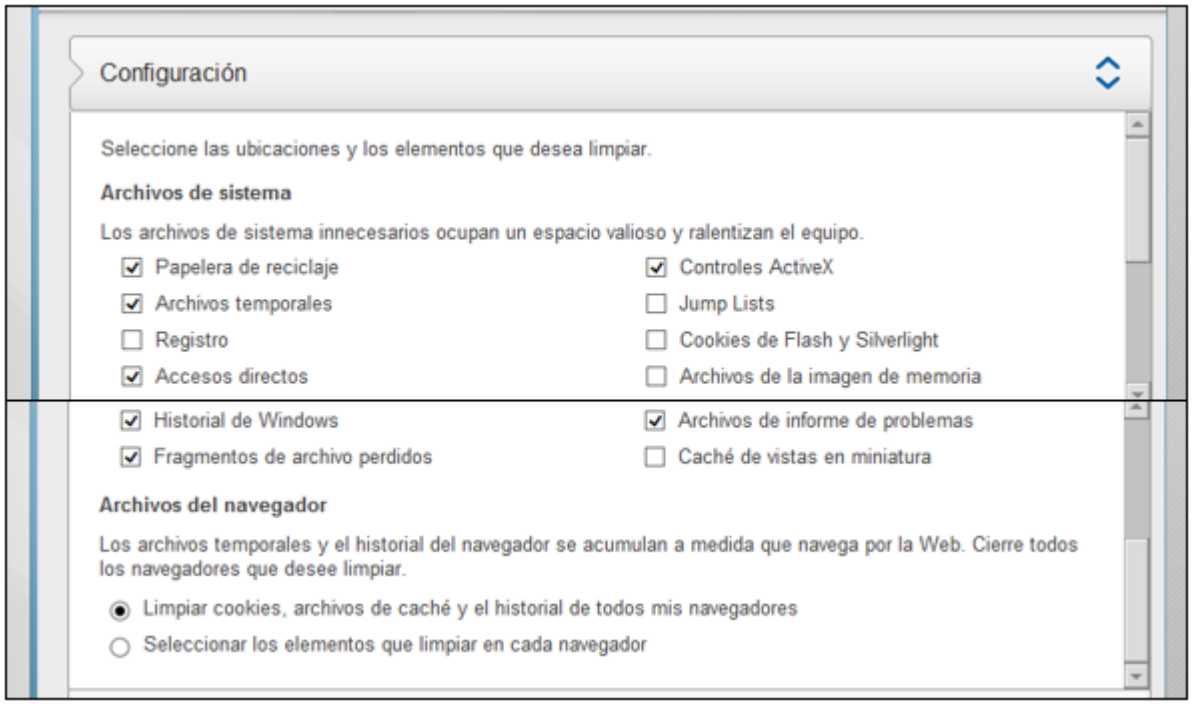
1.1.6.2 QuickClean:

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



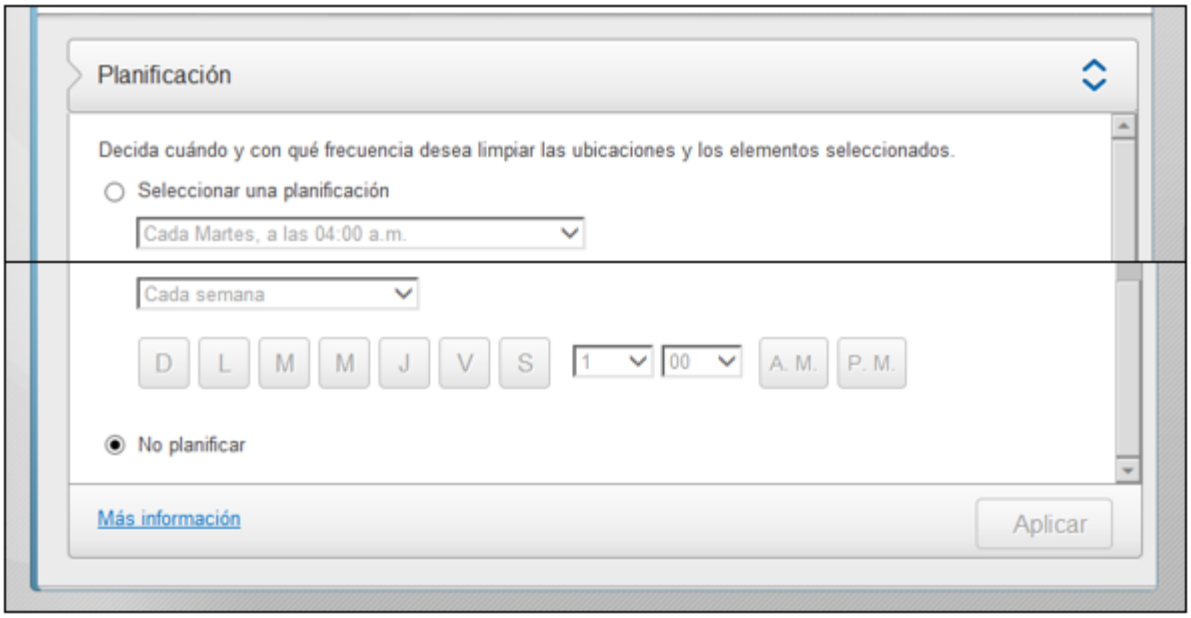
1.1.6.2.1 Configuración

Permite seleccionar las ubicaciones y los elementos que desea limpiar.



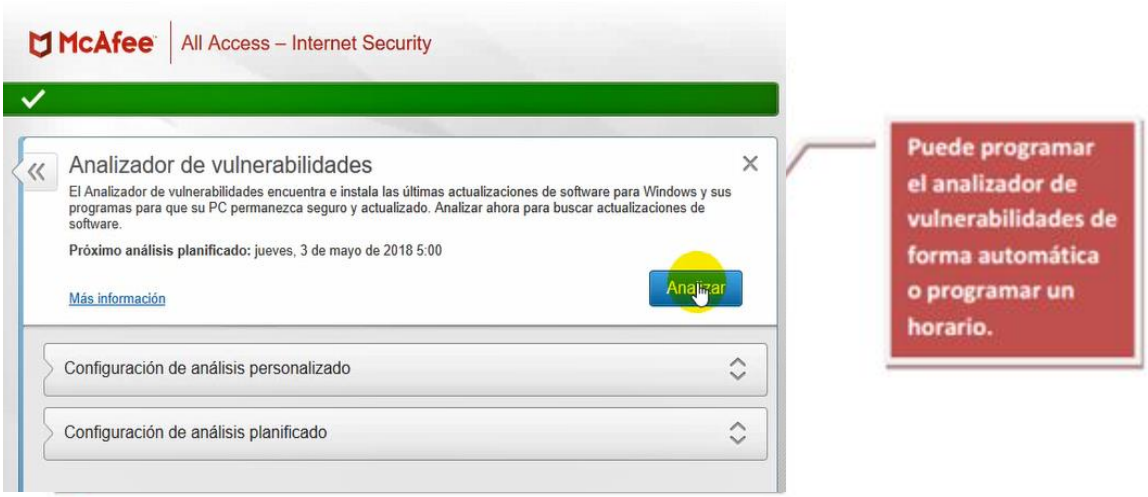
1.1.6.2.2 Planificación

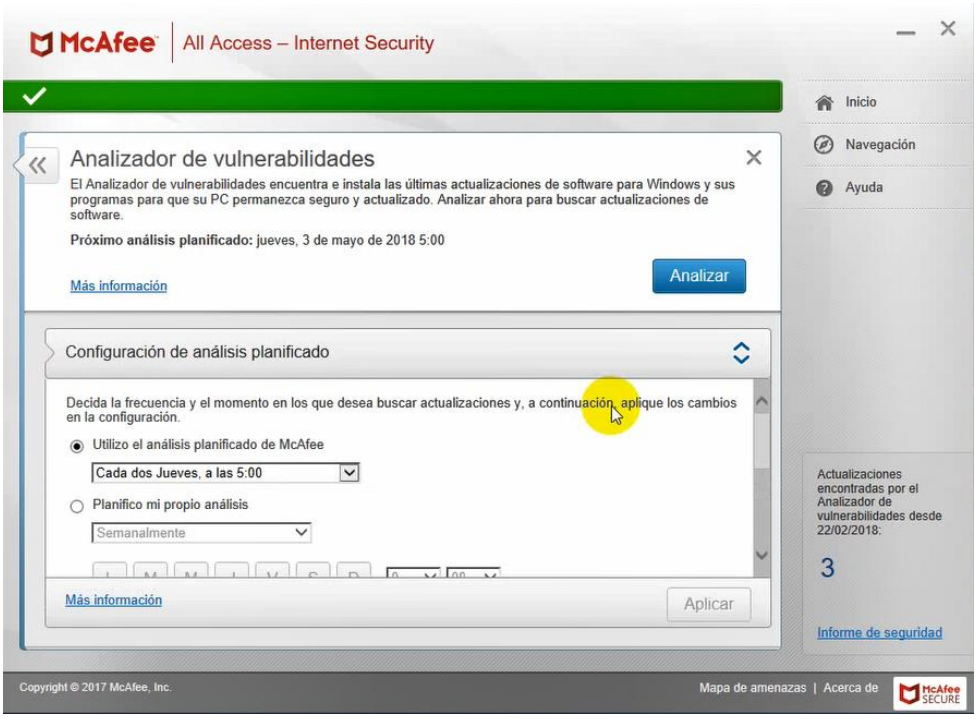
Permite seleccionar la frecuencia en que se desea limpiar los elementos seleccionados.



1.1.6.3 Analizador de vulnerabilidades

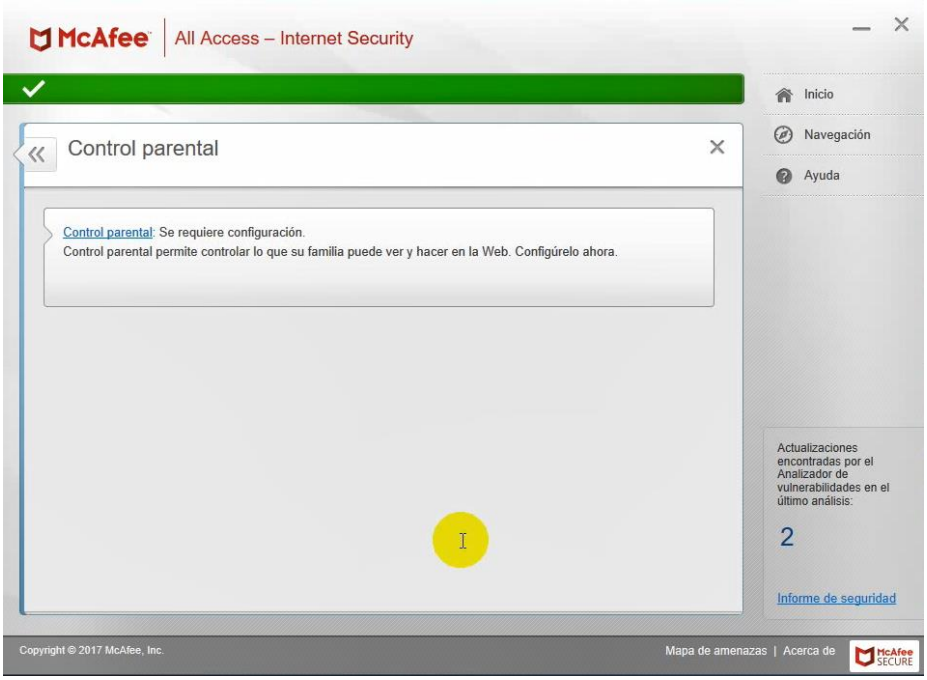
El analizador de vulnerabilidades encuentra e instala las últimas actualizaciones de software para que su equipo permanezca seguro y actualizado.





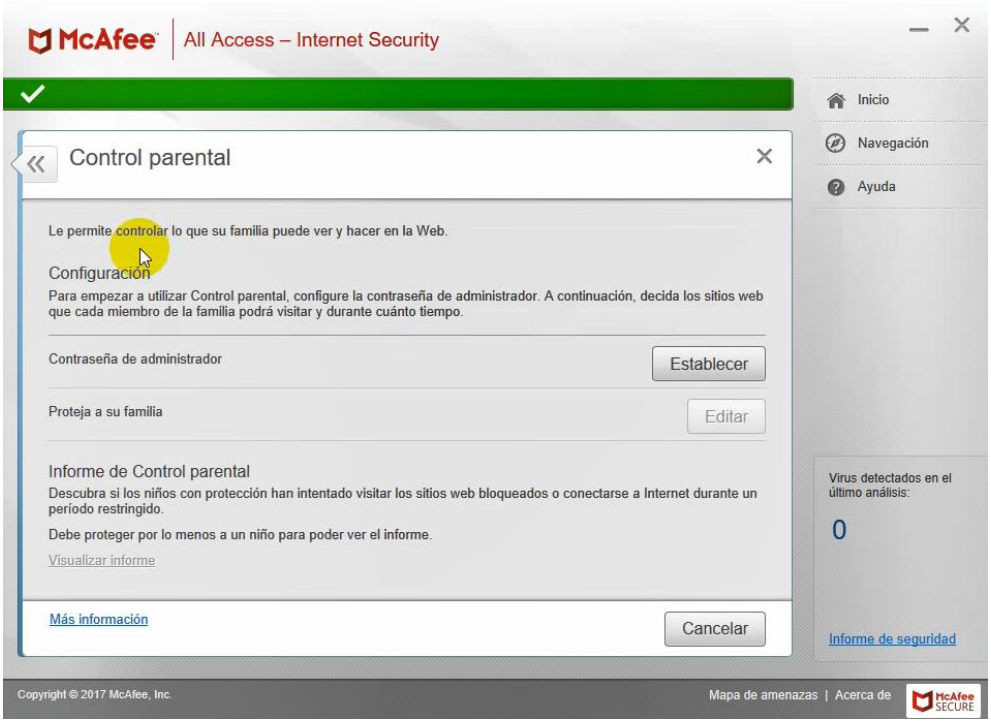
1.1.7 Control parental

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.



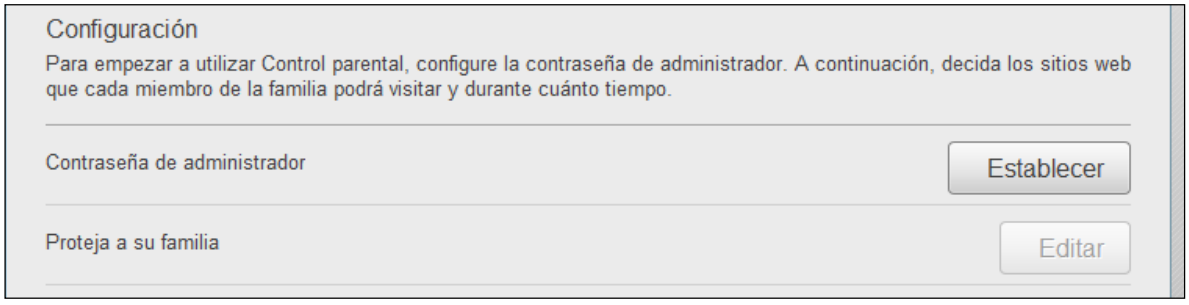
1.1.7.1 Configuración de Control parental:

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.

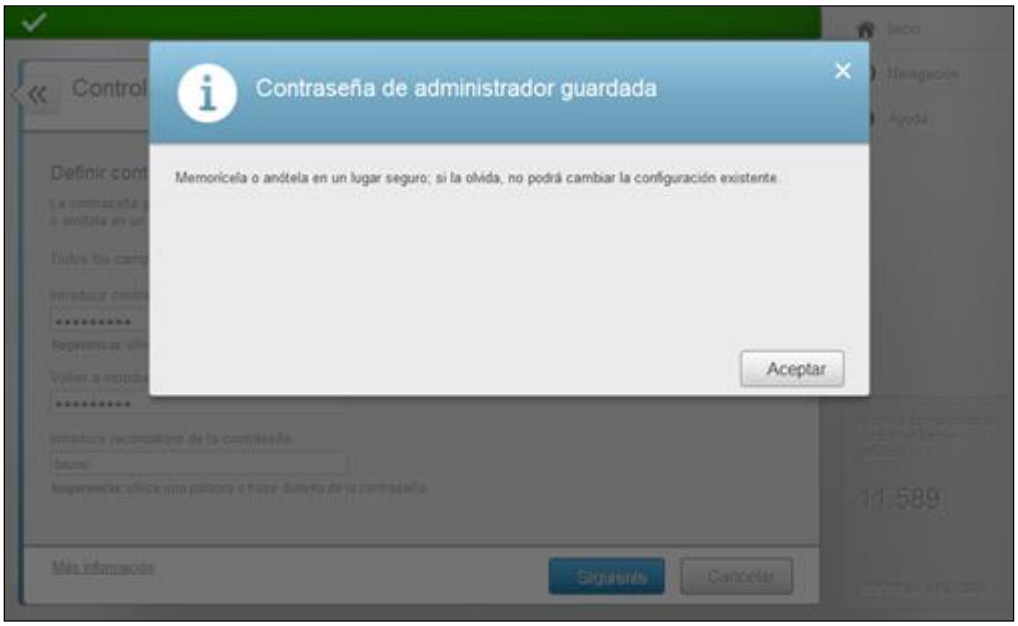


1.1.7.1.1 Definir contraseña de administrador:

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.*

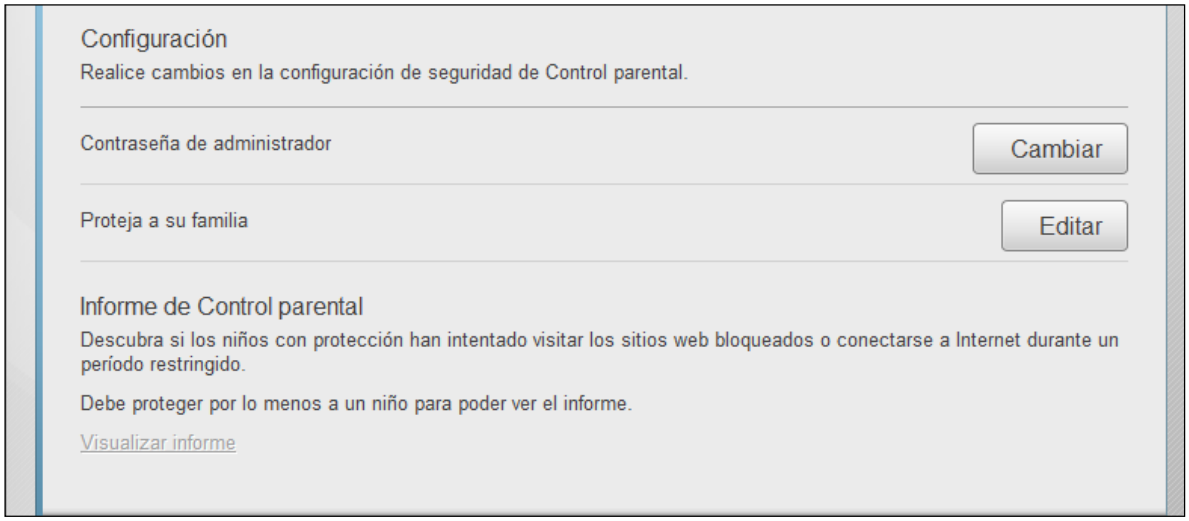


Si olvida la contraseña de administrador una vez asignada no podrá iniciar sesión en el Control parental. Asegúrese de memorizarla, o de apuntarla y guardarla en un lugar seguro; de lo contrario tendrá que reinstalar el software de McAfee para restablecer la contraseña.

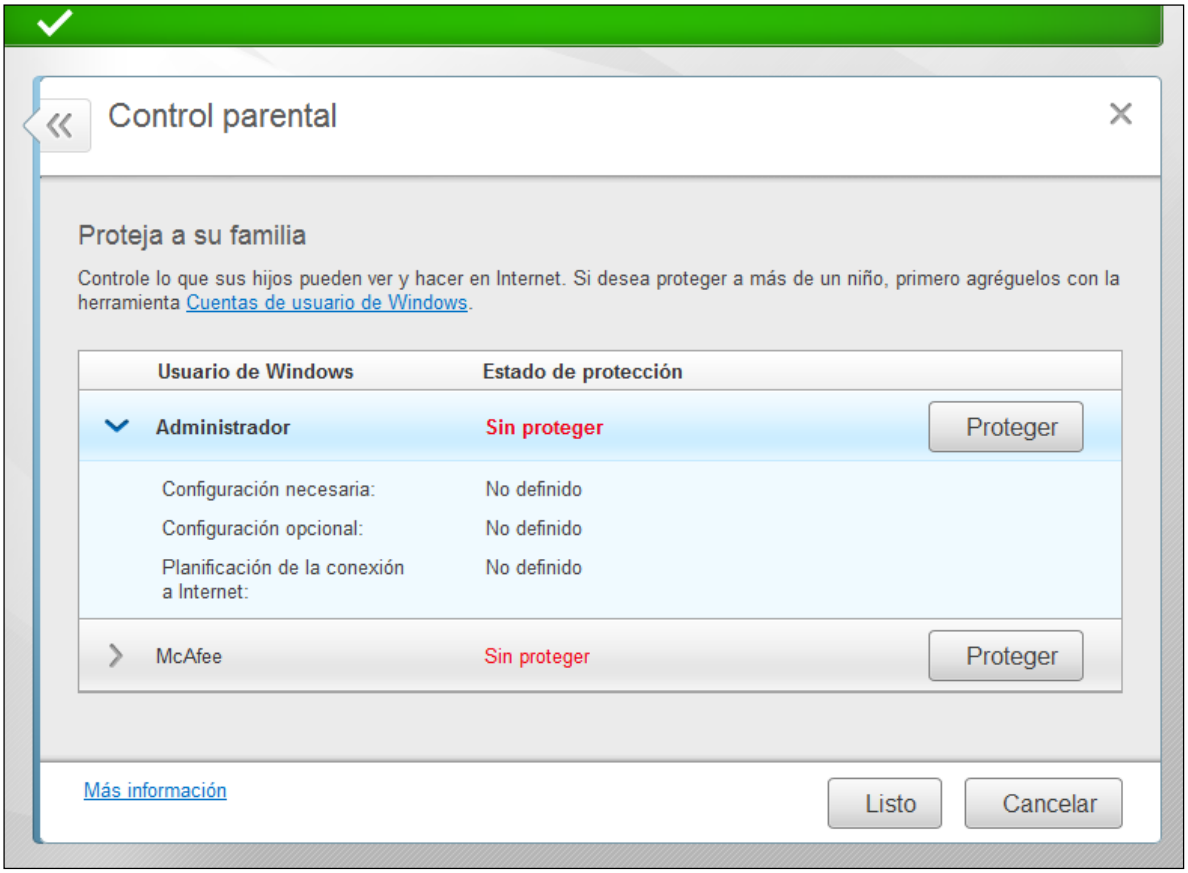
1.1.7.1.2 ***Protección de los usuarios:***

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)

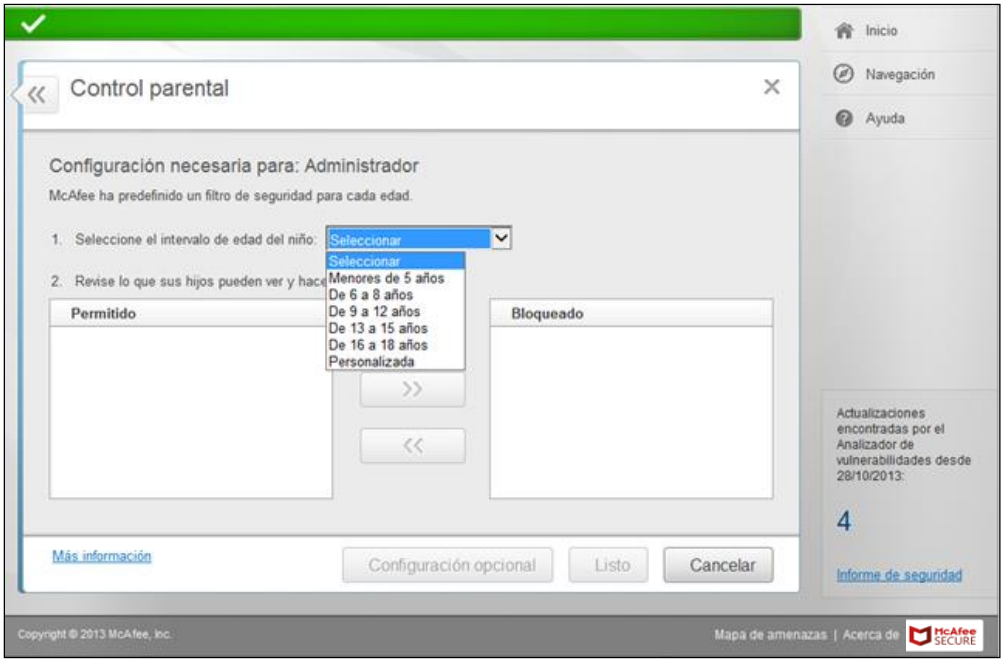


Ingrese la contraseña de administrador y presione *Enter.* Los usuarios que aparecen a continuación son las mismas cuentas de usuario de Windows que se definieron previamente en el equipo. (Para verificar como se crean usuarios en Windows)



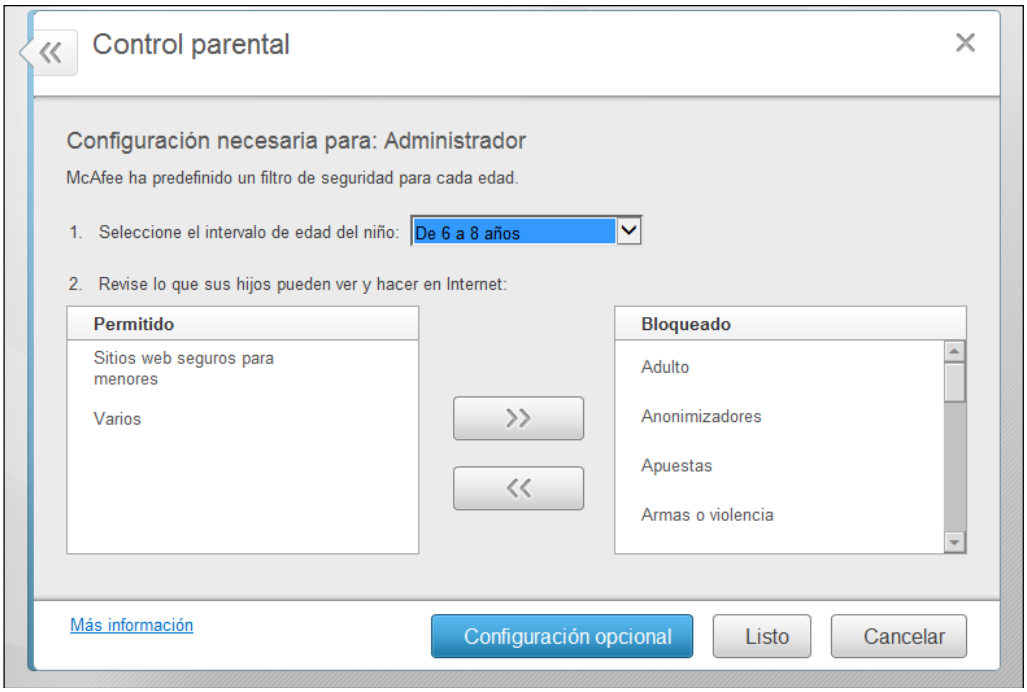
Si agrega un usuario mediante el Panel de control, Cuentas de usuario, debe cerrar el Centro de Seguridad de McAfee y, a continuación, al volverlo abrir podrá asignarle valores de configuración de protección en Control parental.

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.*



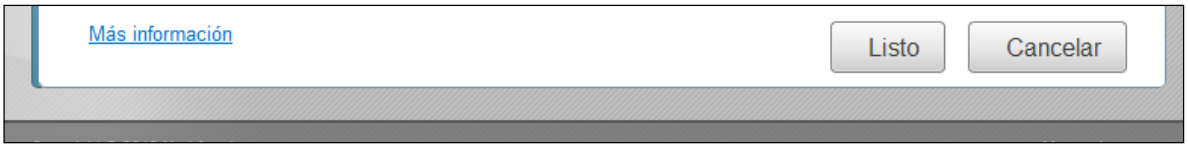
Estos listados pueden personalizarse, agregando o quitando categorías, tanto en *Permitidos* y *Bloqueados.* Es posible quitar *Juegos* de *Permitido, se* selecciona esta categoría y se presiona el botón que apunta a *Bloqueado* (8).

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

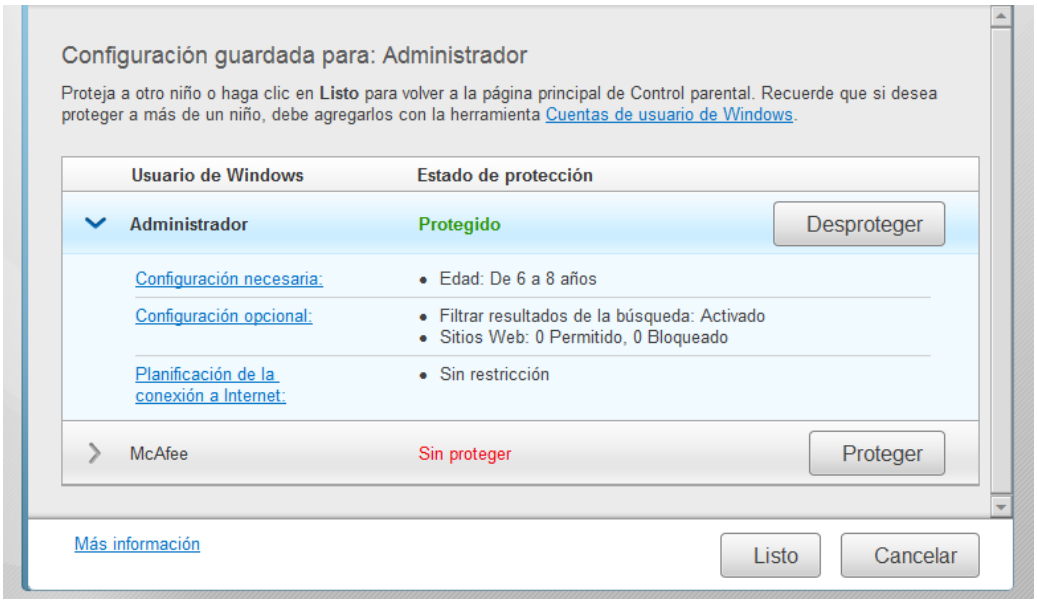
1.1.7.1.4 *Uso de la búsqueda segura:*

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).

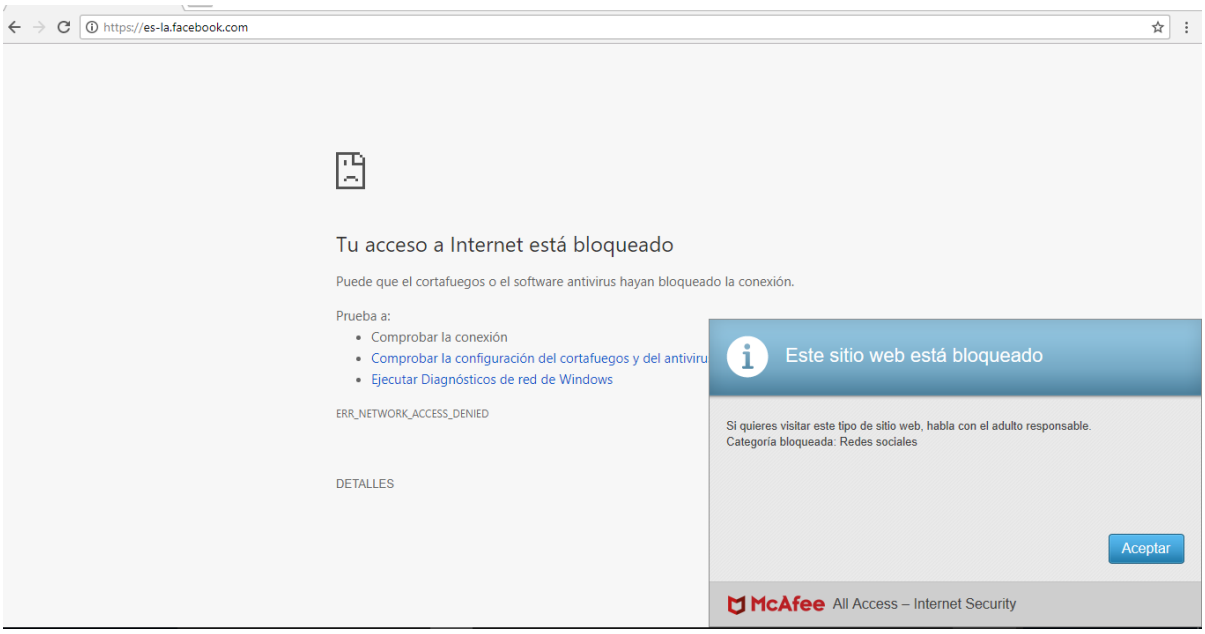


Con el Control parental, la búsqueda segura se activa de forma predeterminada cuando configuramos la protección de los usuarios.

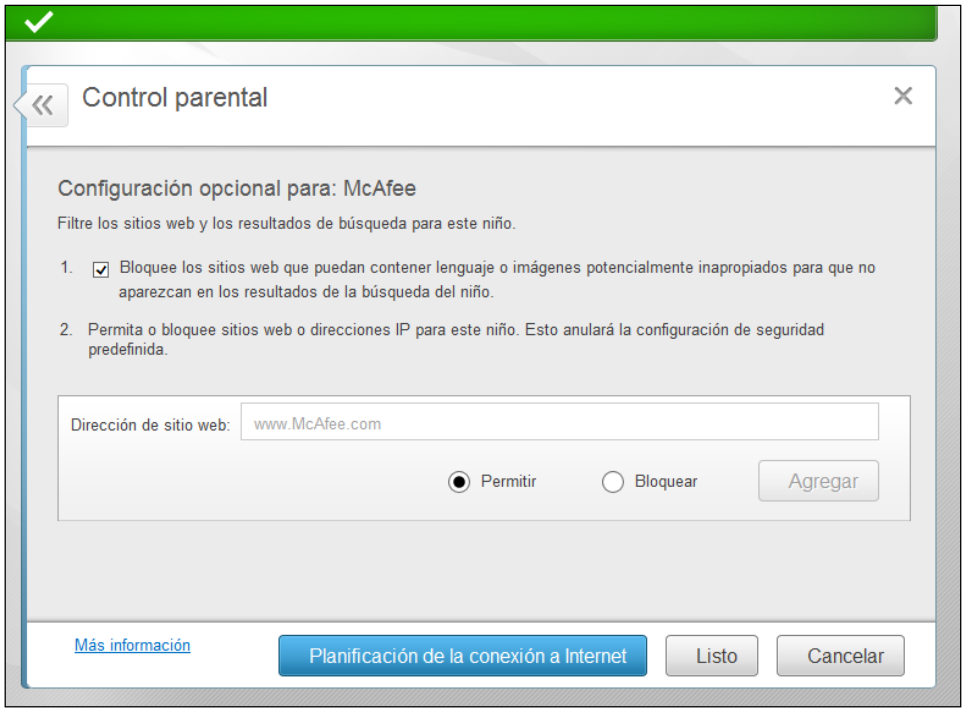


1.1.7.1.5 *Autorizar y bloquear sitios web:*

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

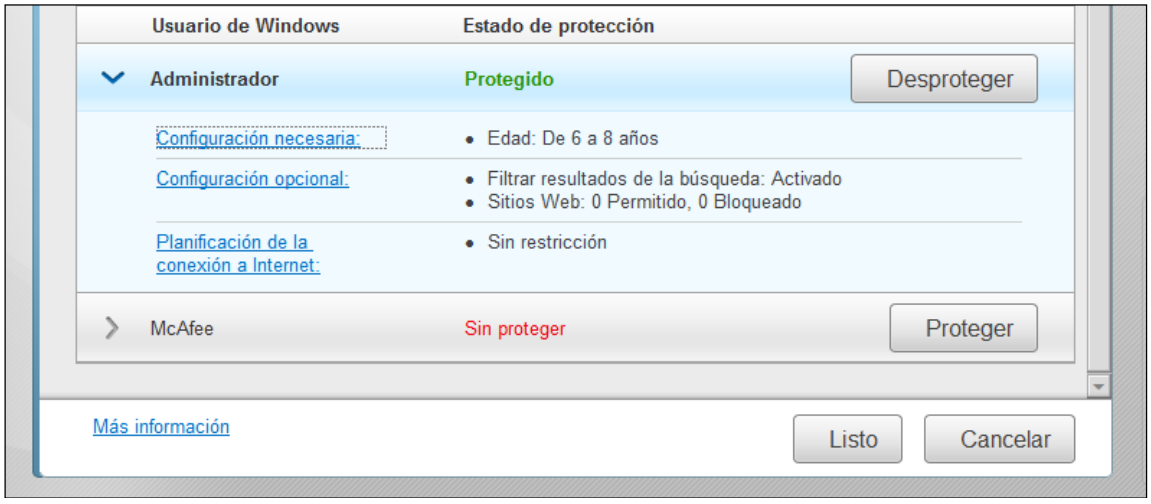


Si desea que un usuario pueda visitar un sitio web específico, puede agregar la dirección web correspondiente en la lista de filtros (10) y definir el nivel de permiso como *Permitir* (11) y *Agregar* (13). Si, por el contrario, no desea que el usuario tenga acceso a un sitio web específico, puede agregar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



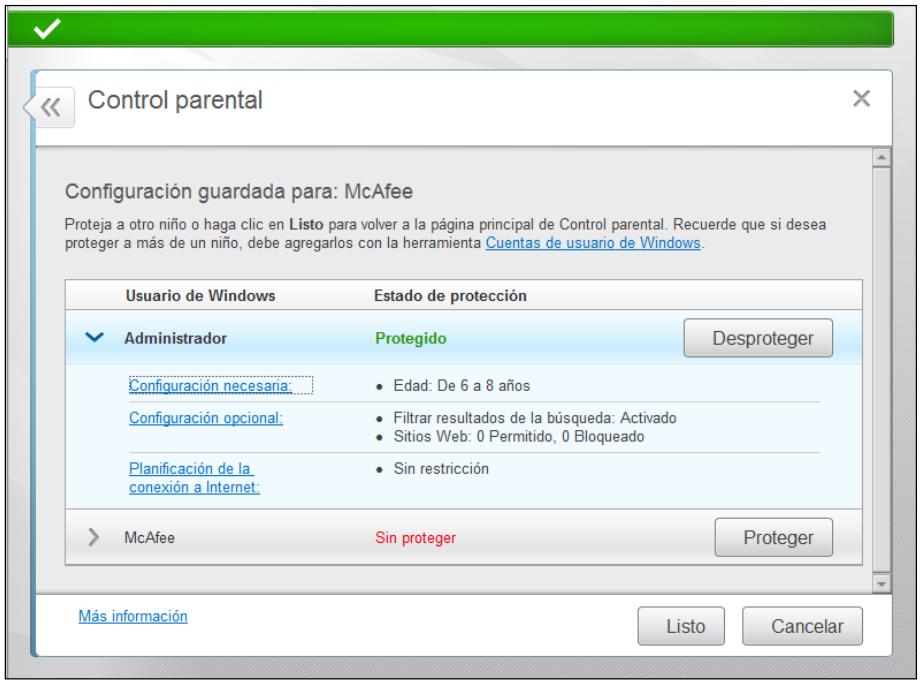
Los sitios web y los permisos que se incorporen a esta lista, tanto como sitios permitidos y bloqueados, anularán los permisos definidos por grupos de edad y categorías de contenido.

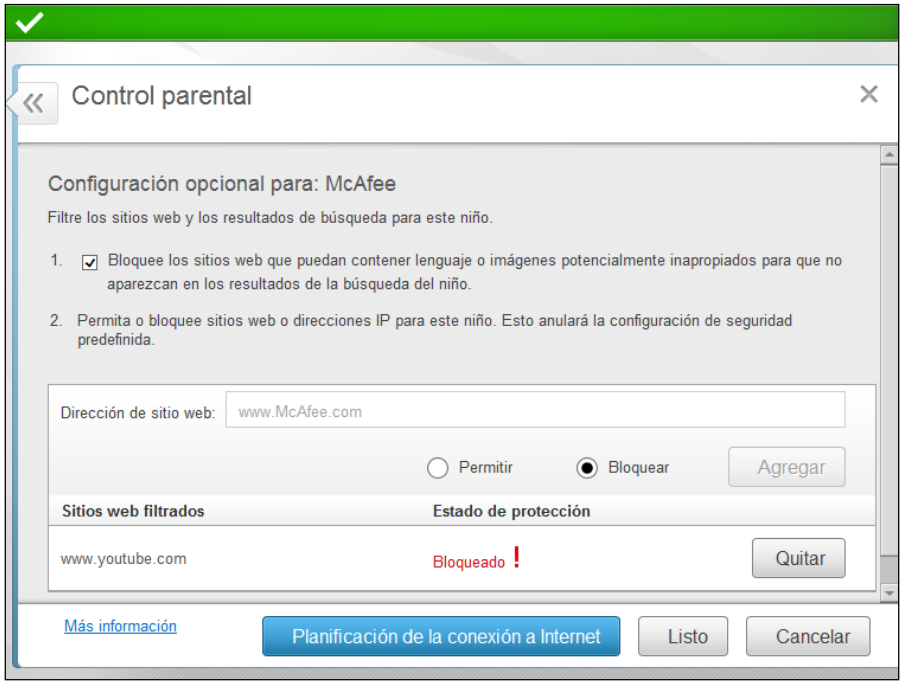
Si desea que el *Control Parental* deje de filtrar un sitio Web específico, puede eliminarlo en cualquier momento, presionando *Quitar*.

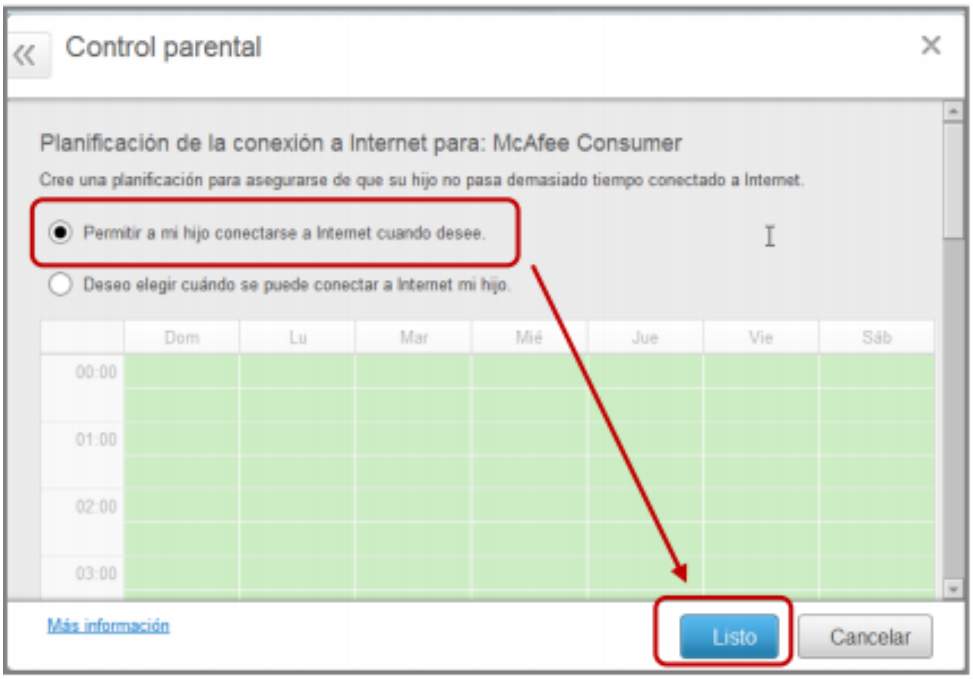


1.1.7.1.6 *Control del tiempo de navegación en la web:*

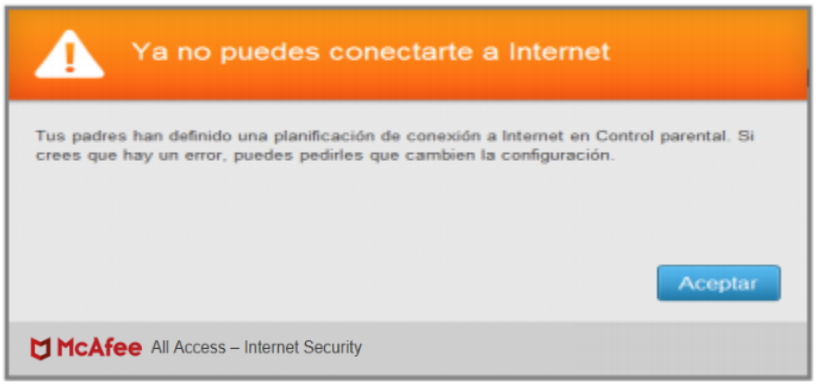
De forma predeterminada, todos los usuarios podrán navegar por Internet cuando deseen. Sin embargo, si le preocupa que un usuario dedique demasiado tiempo a navegar por la web, podrá controlar el acceso a ésta y establecer un límite de tiempo para ello. Para ello, continuamos la configuración del *Control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





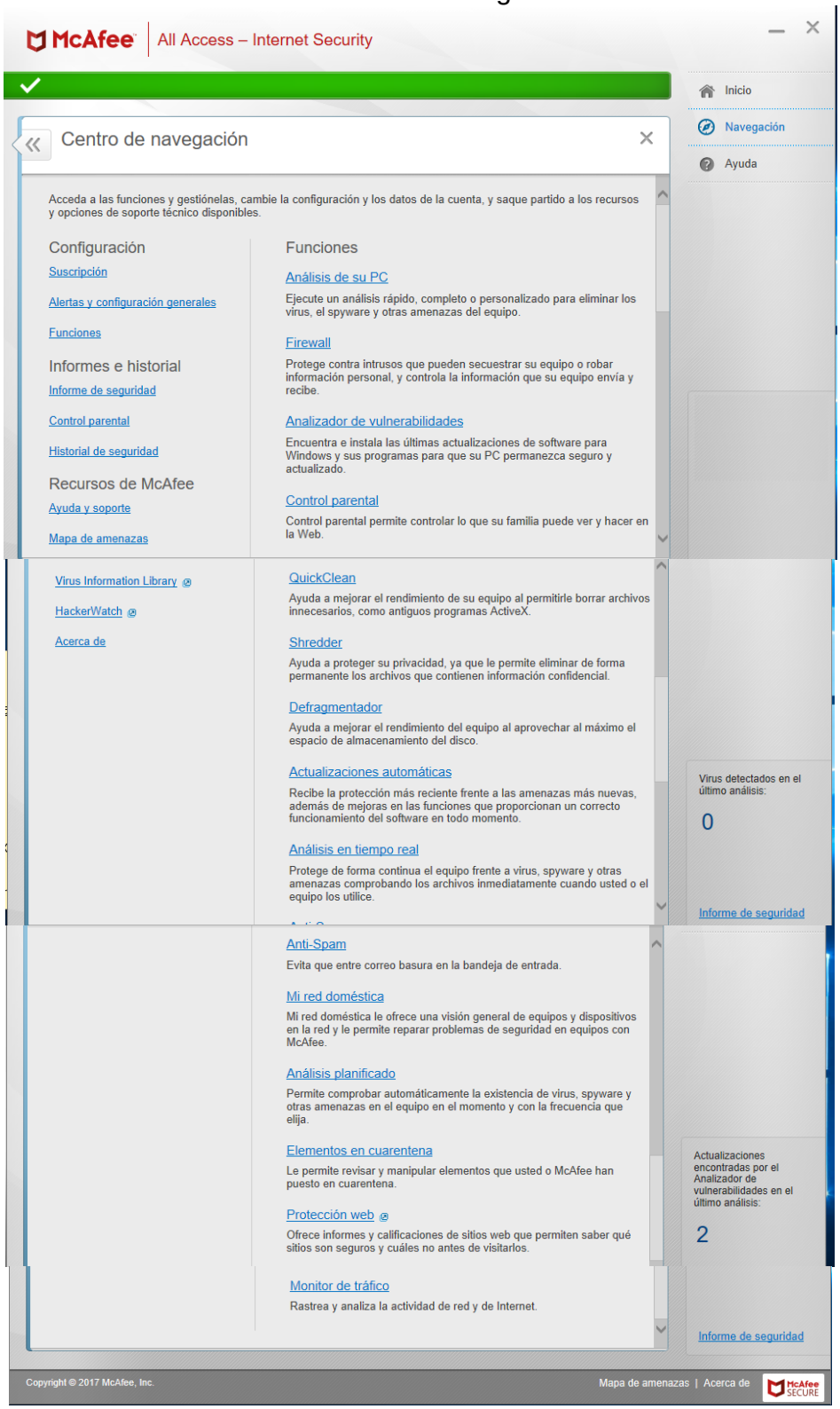


Si está en verde indicará el tiempo permitido, si está en color blanco indicará el tiempo bloqueado



2. Centro de navegación:

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

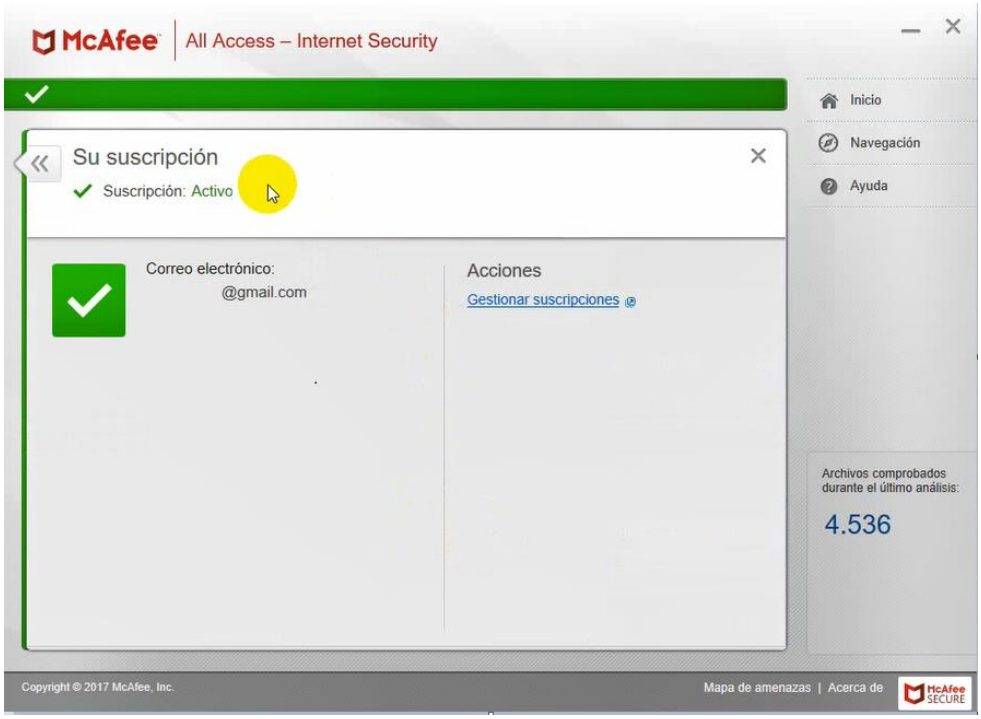


2.1 Configuración:

Permite ingresar a algunas funciones para configurar la consola.

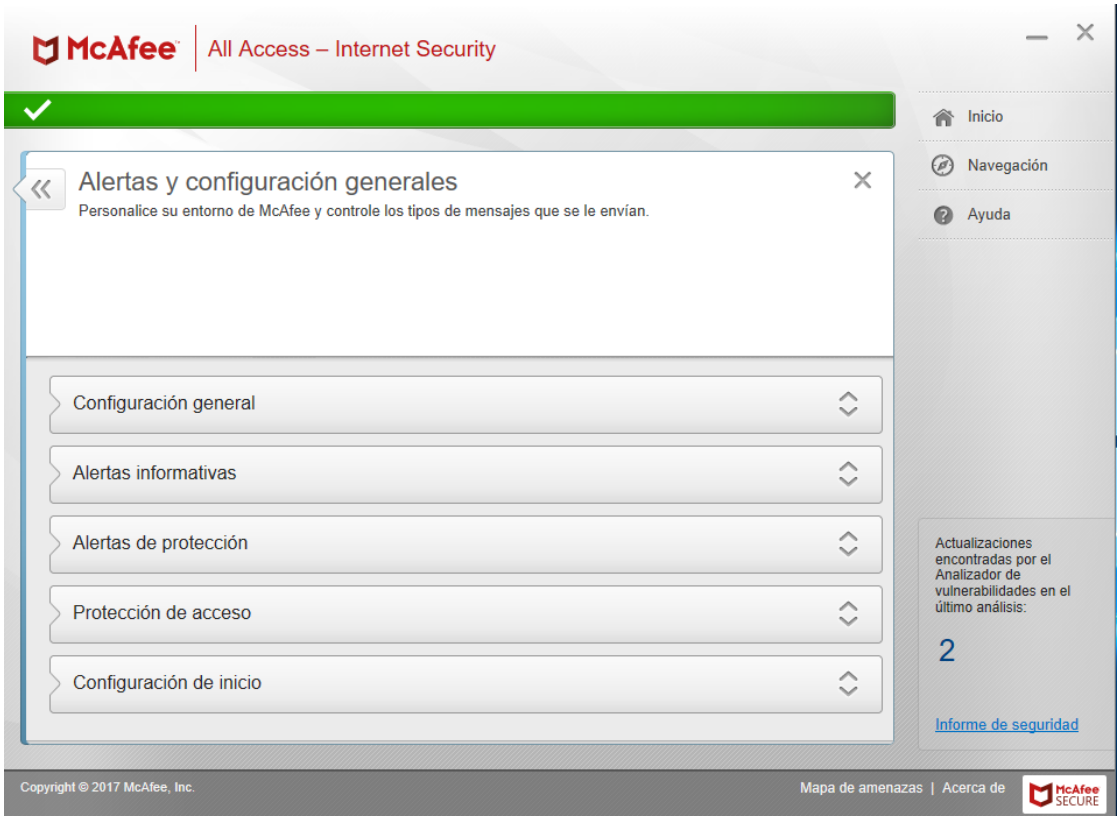
2.1.1 Suscripción:

Permite verificar el estado de la suscripción.

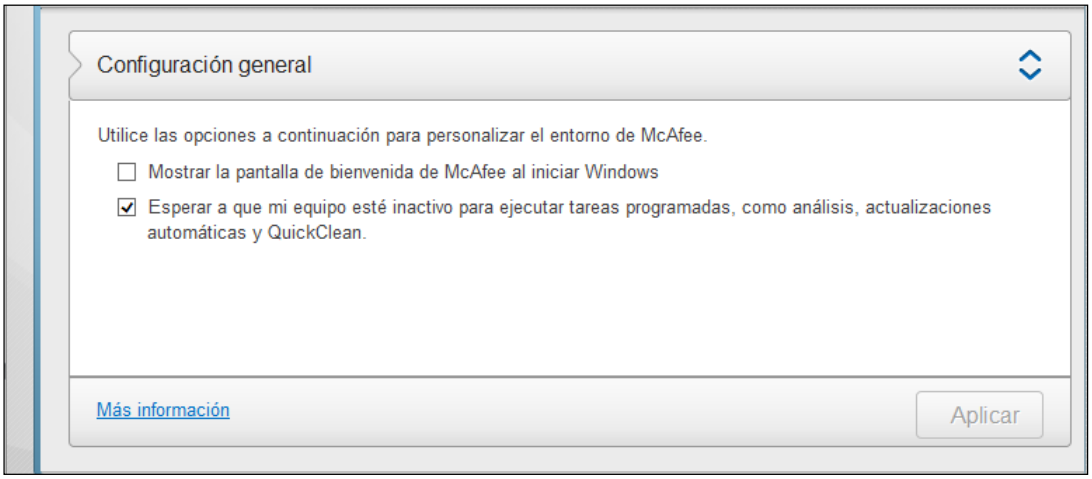


2.1.2 Alertas y configuración generales:

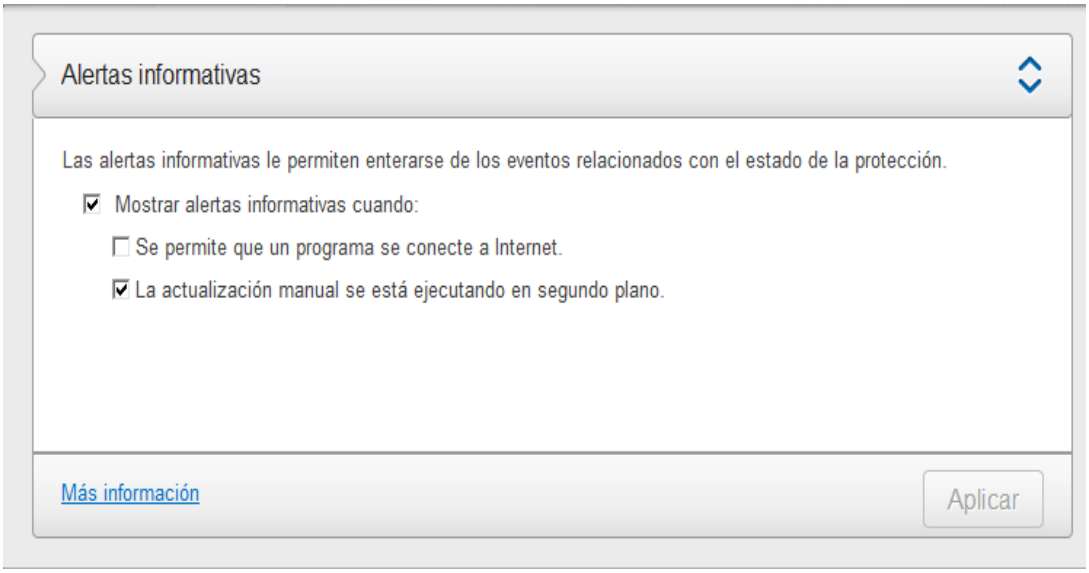
Permite personalizar su entorno de McAfee y controlar los tipos de mensajes que le envían.



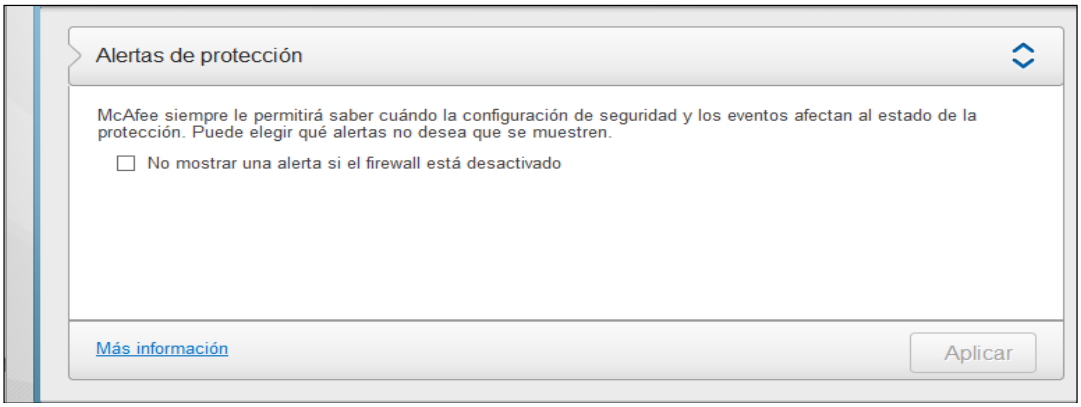
2.1.2.1 Configuración General:



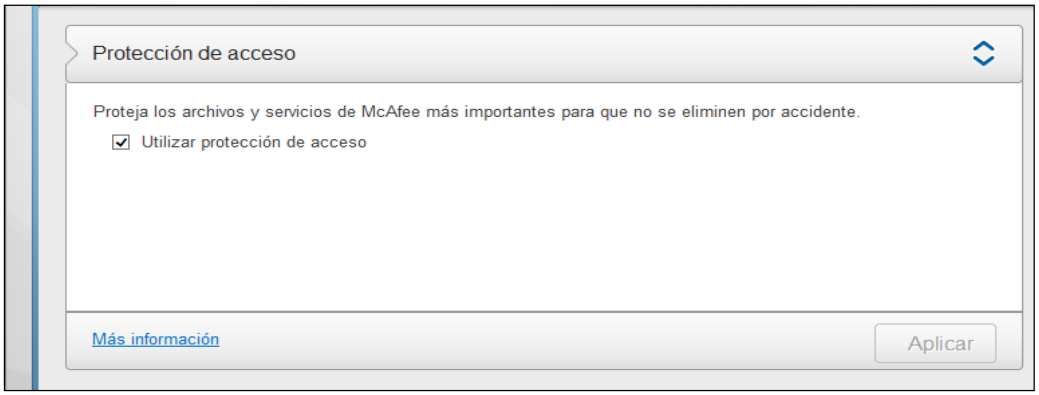
2.1.2.2 Alertas informativas:



2.1.2.3 Alertas de protección:

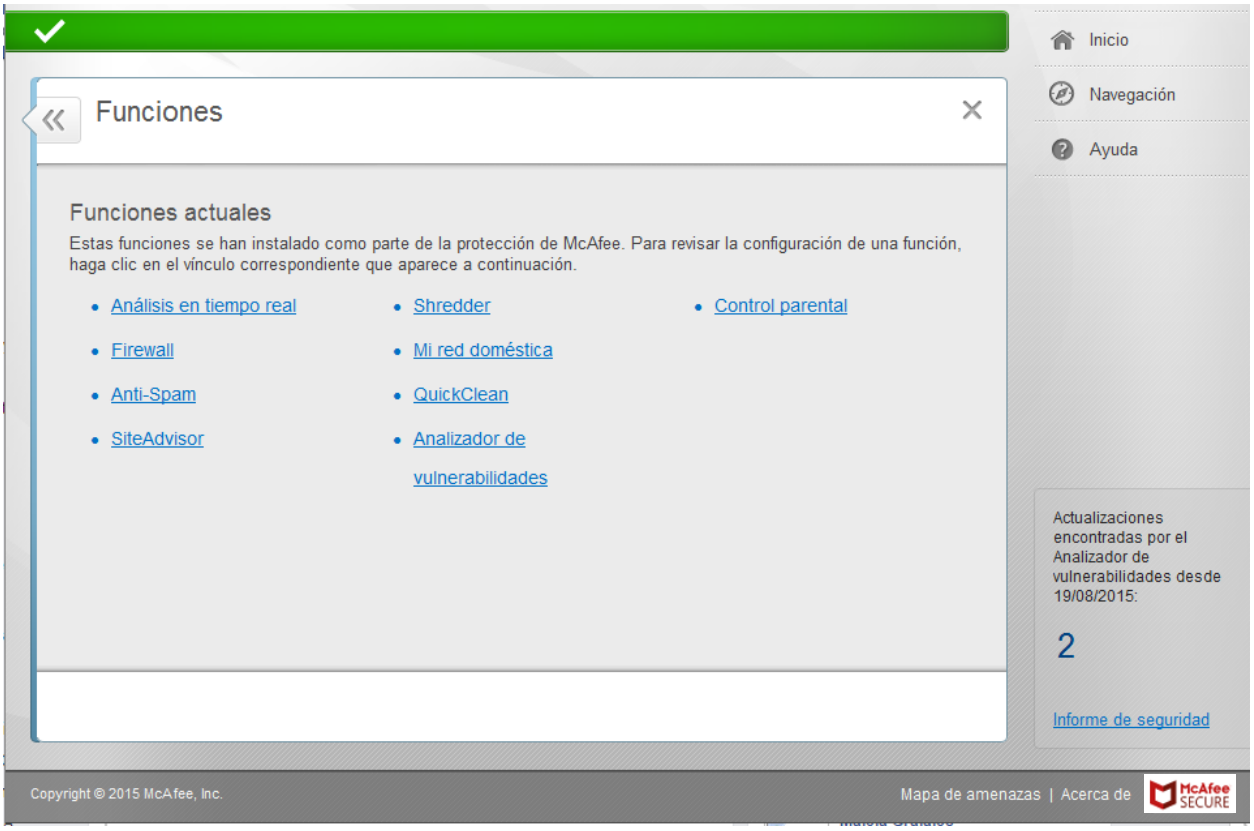


2.1.2.4 Protección de acceso



2.1.3 Funciones:

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

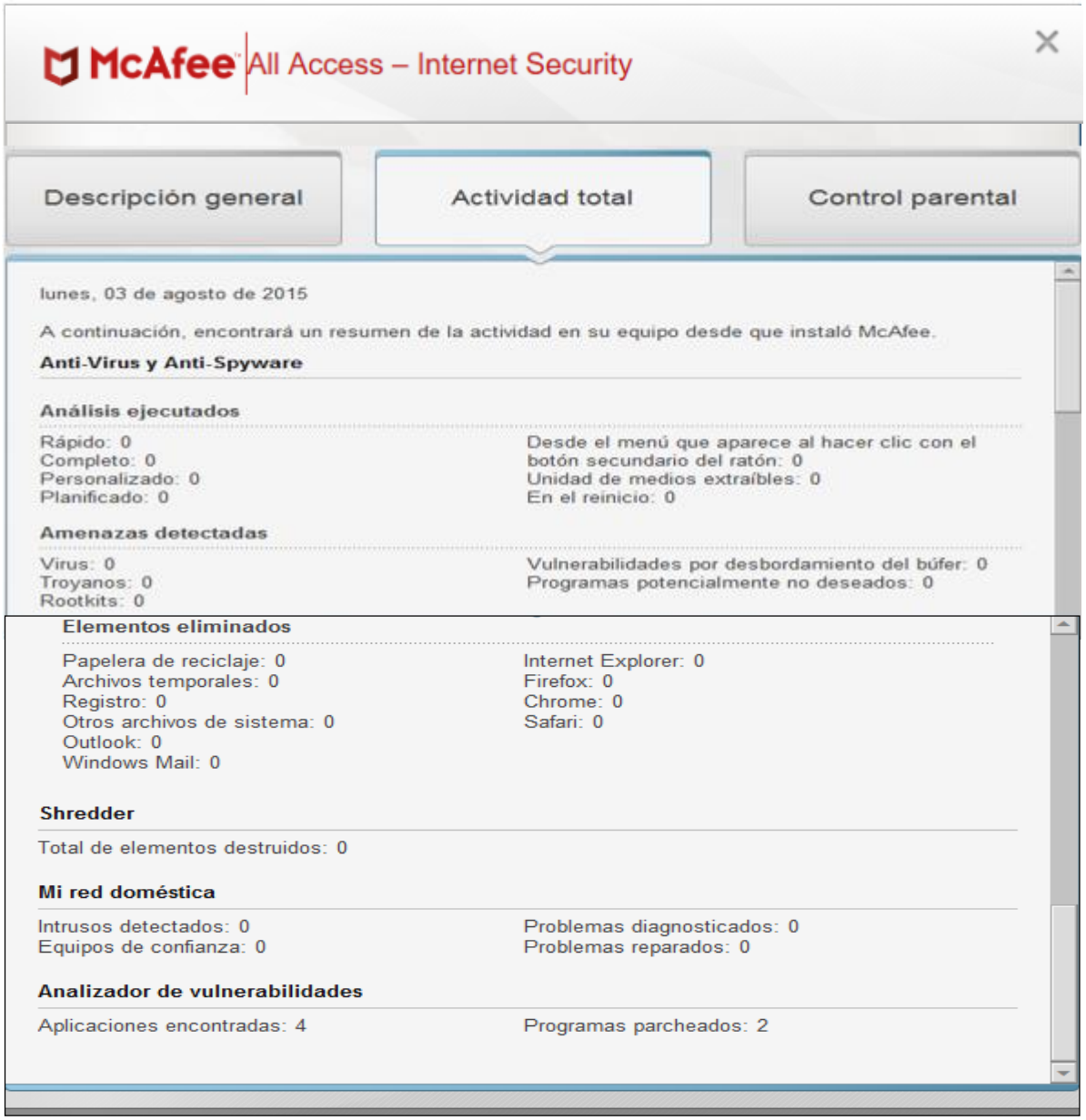


2.2 Informes e historial:

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

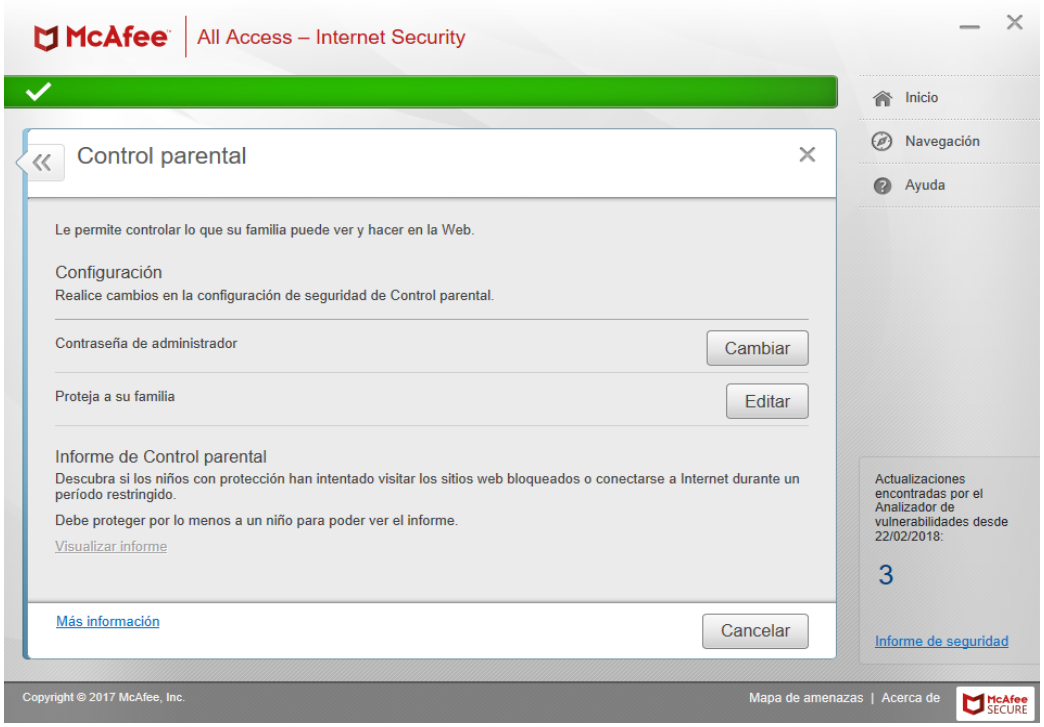
2.2.1 Informe de seguridad:

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
Completo: 0
Personalizado: 0
Planificado: 0
Desde el menú que aparece al hacer clic con el botón secundario del ratón: 0
Unidad de medios extraíbles: 0
En el reinicio: 0
Amenazas detectadas
Virus: 0
Troyanos: 0
Rootkits: 0
Vulnerabilidades por desbordamiento del búfer: 0
Programas potencialmente no deseados: 0
Elementos eliminados
Papelera de reciclaje: 0
Archivos temporales: 0
Registro: 0
Otros archivos de sistema: 0
Outlook: 0
Windows Mail: 0
Internet Explorer: 0
Firefox: 0
Chrome: 0
Safari: 0
Shredder
Total de elementos destruidos: 0
Mi red doméstica
Intrusos detectados: 0
Equipos de confianza: 0
Problemas diagnosticados: 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.



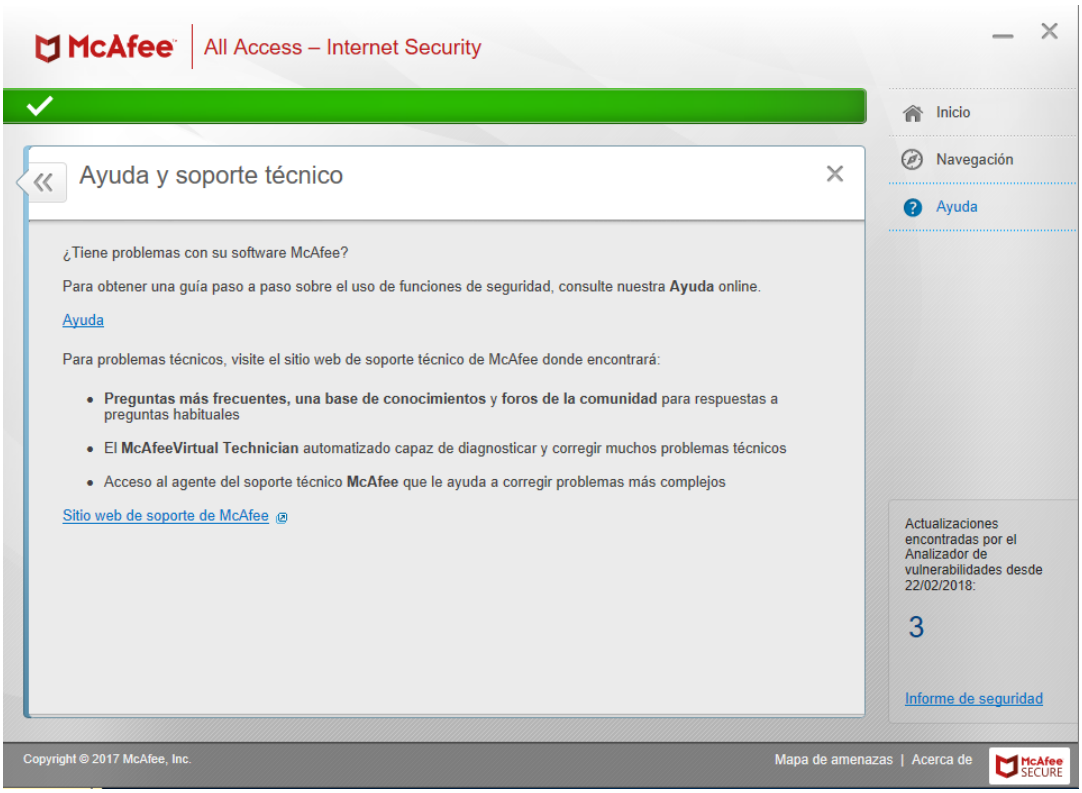
2.2.3 Historial de seguridad:

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

3. Recursos de McAfee:

3.1 Ayuda de Soporte:

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



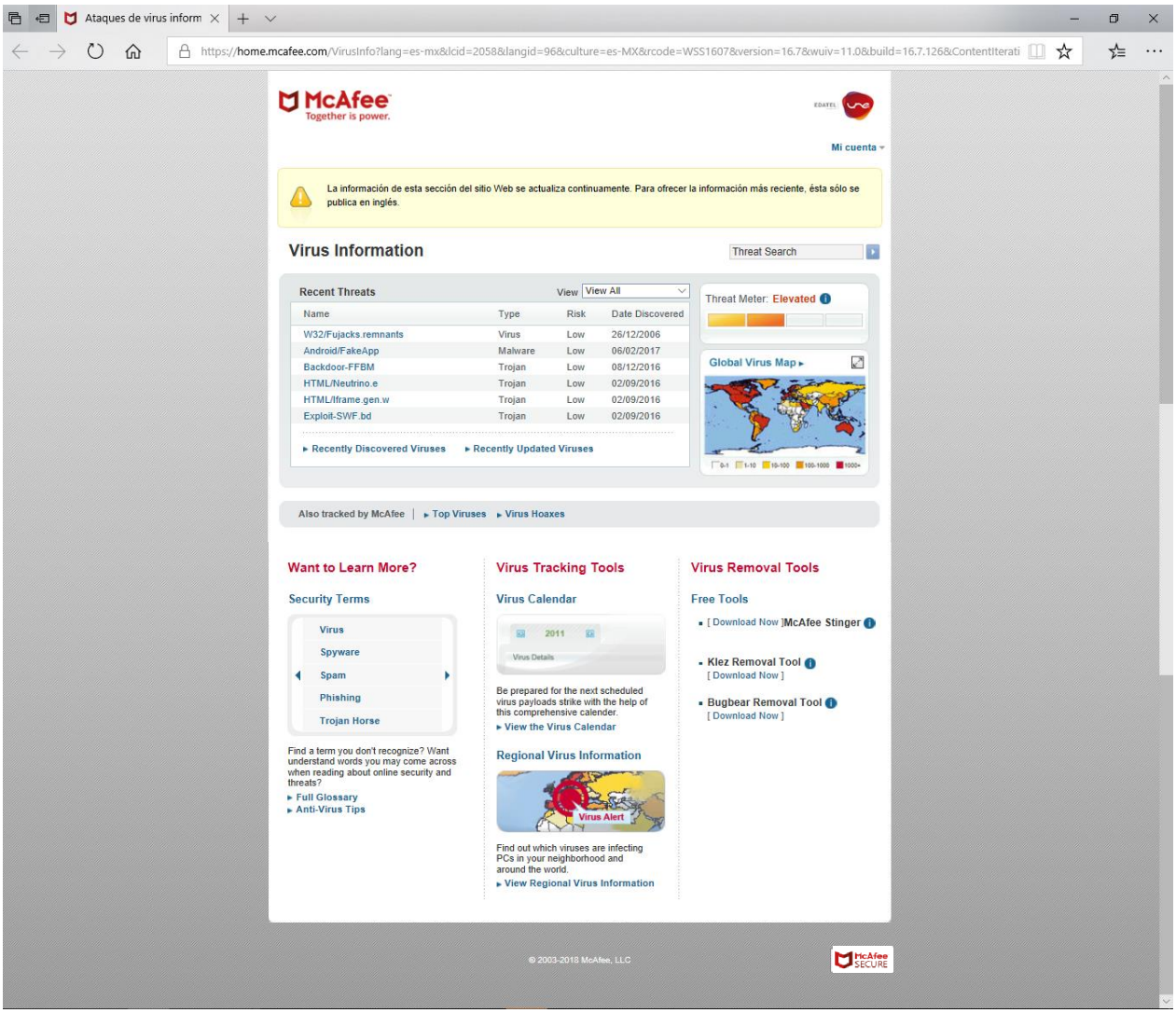
Se le recomienda consultar a su operador de confianza cualquier inquietud que esta guía y/o centro de navegación le genere.

3.2 Mapa de amenazas:

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

3.3 Virus information Library:

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



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.